TREND MICRO™

Remote Manager

Benutzerhandbuch

Protected Cloud

Trend Micro Incorporated behält sich das Recht vor, Änderungen an diesem Dokument und den hierin beschriebenen product/service ohne Vorankündigung vorzunehmen. Lesen Sie vor der Installation und Verwendung der product/service die Readme-Dateien, die Anmerkungen zu dieser Version und/oder die neueste Version der entsprechenden Benutzerdokumentation durch. Sie finden diese Dokumente auf der Trend Micro Website unter:

http://docs.trendmicro.com/de-de/home.aspx

Trend Micro, das Trend Micro T-Ball-Logo und Worry-Free sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Produkt- oder Firmennamen können Marken oder eingetragene Marken ihrer Eigentümer sein.

© 2014 Trend Micro Incorporated. Alle Rechte vorbehalten.

Dokument-Nr.: APGM36800/141125

Release-Datum: Dezember 2014

Geschützt durch U.S. Patent-Nr.: Patent angemeldet.

In dieser Dokumentation werden die wesentlichen Funktionen von product/service erläutert und/oder sind die Installationshinweise für eine Produktionsumgebung enthalten. Lesen Sie die Dokumentation vor der Installation und Verwendung von product/service aufmerksam durch.

Ausführliche Informationen über die Verwendung bestimmter Funktionen von product/service finden Sie im Trend Micro Online-Hilfe-Center und/oder der Trend Micro Knowledge Base.

Trend Micro ist stets bemüht, die Dokumentation zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder einem anderen Dokument von Trend Micro wenden Sie sich bitte an docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

http://www.trendmicro.com/download/documentation/rating.asp

Inhaltsverzeichnis

Vorwort

Vorwort vii

Info über Trend Micro viii

Zielpublikum viii

Textkonventionen viii

Kapitel 1: Einführung

Trend Micro Remote Manager 1-2

Funktionen 1-4

- Integrierte Plattform 1-5
- Dashboard-Widgets 1-5
- Anpassbare Einstellungen für neue Konten 1-5
- Bedrohungsstatus 1-5
- Systemstatus 1-7
- Lizenzstatus 1-8
- Netzwerkverwaltung 1-8
- Berichte 1-8
- Integration in Tools von Drittanbietern 1-9
- Übermittlung von Feedback 1-9

Unterstützte Produkte 1-9

- Worry-Free Business Security Suite 1-10
- Hosted Email Security 1-11
- Cloud Edge 1-11
- InterScan Web Security as a Service 1-12
- Tools von Drittanbietern 1-15

Neues 1-22

Globale Infrastruktur 1-26

Wichtige Begriffe 1-28

Kapitel 2: Erste Schritte

Browser-Anforderungen 2-2
URL der Trend Micro Remote Manager Web-Konsole zu den vertrauenswürdigen Sites hinzufügen 2-2
SSL-Zertifikat mit Internet Explorer 9 ermitteln 2-3
Auf die Plattform zugreifen 2-3
Koordination mit dem Kunden 2-4

Kapitel 3: Die Web-Konsole verstehen

Das Web-Konsolen-Banner 3-2
Anleitungsvideos und bewährte Methoden 3-4
Hauptmenü 3-5
Mein Konto 3-6
Das Dashboard verstehen 3-7
Dashboard Statusfenster 3-7
Registerkarten und Widgets 3-8
Produkt-/Service-Information 3-22

Kapitel 4: Infrastruktur einrichten

Überblick über die Installation der Infrastruktur 4-2
Worry-Free Business Security Standard und Worry-Free Business Security Advanced 4-2
Hosted Email Security und Worry-Free Business Security Services 4-2
InterScan Web Security as a Service (IWSaaS) 4-2
ConnectWise 4-3
Kaseya 4-3
Autotask 4-3
Produkte hinzufügen 4-4
Kunden hinzufügen 4-4
Trend Micro Produkte bei Trend Micro Remote Manager registrieren 4-8
Produkte anderer Hersteller in Trend Micro Remote Manager integrieren 4-16

Kapitel 5: Kunden verwalten

Kunden 5-2
Neue Kunden hinzufügen 5-2
Konten zuweisen 5-7
Produktlizenz überprüfen 5-9
Produkte/Services hinzufügen 5-9
Kontakte 5-10
Kundenliste filtern 5-10

Kapitel 6: Agents verwalten

Agents über die Remote Manager Web-Konsole verwalten 6-2
Verbindung zwischen Agent und Server überprüfen 6-2
Agent-Status 6-2
Agent-Befehle absenden 6-4
Agent-Details anzeigen 6-5

Agents über den verwalteten Server verwalten 6-6
Agent-Statusmeldungen 6-6
Die Agent-GUID auf dem verwalteten Server ändern 6-7
Agent-Konfigurationstool verwenden 6-8
Agent-Konfiguration 6-8

Agent-Einstellungen sichern und wiederherstellen 6-12
Einstellungen sichern 6-12
Einstellungen wiederherstellen 6-13

Build-Nummer des Agents suchen 6-14
Über die Remote Manager Web-Konsole 6-14
Im Agent 6-14

Speicherorte der Agent-Protokolle und -Konfigurationsdateien 6-15

Das Agent-Fehlerprotokoll aktivieren 6-15

Agents entfernen 6-15
Agents lokal entfernen 6-16

Kapitel 7: Lizenzen verwalten

Arbeitsplatzzuordnungen hinzufügen 7-2

Lizenzen verlängern 7-3

Kapitel 8: Einstellungen verwalten

Benachrichtigungen konfigurieren 8-2
Konsoleneinstellungen konfigurieren 8-3
Standardeinstellungsvorlagen konfigurieren 8-4

Kapitel 9: Ereignisse verwalten

Ereignisse verwalten 9-2
Ereignisse anzeigen 9-4
Ereignistypen 9-5
Details des Ausbruchsschutzstatus 9-5
Details des Antiviren-Status 9-7
Details des Anti-Spyware-Status 9-9
Details des Anti-Spam-Status 9-11
Details des Netzwerkvirenstatus 9-11
Details des Web-Reputation-Status 9-12
Details des Verhaltensüberwachungsstatus 9-13
Details des URL-Filter-Status 9-13
Details der Gerätesteuerung 9-14
Smart Scan 9-14
Komponenten-Update 9-15
Speichernutzung 9-16

Kapitel 10: Berichte

Überblick über Berichte 10-2
Berichte erstellen 10-3
Berichtvorlagen erstellen 10-3
Berichte anzeigen 10-7
Berichte bearbeiten 10-7
Berichte herunterladen und versenden 10-7
Berichte abonnieren 10-8

Kapitel 11: Fehlerbehebung und bekannte Probleme

Fehlerbehebung in der Trend Micro Remote Manager Web-Konsole 11-2
Zugriffsprobleme ... 11-2
Domänenansicht nach Installation des Agents nicht sichtbar ... 11-2
Knoten in Struktur kann nicht erweitert werden ... 11-3
Seite kann nicht angezeigt werden ... 11-4
Fehlerhafte Informationen auf dem Dashboard ... 11-4
Es können keine Befehle übermittelt werden ... 11-5
Agent-Status ist ungewöhnlich ... 11-5
Agent funktioniert unter Verwendung einer vorhandenen GUID nicht ordnungsgemäß nach 11-6

Fehlerbehebung für den Agent ... 11-6
Probleme mit dem Agent ... 11-6
Es konnte keine Verbindung zum Server hergestellt werden ... 11-8
Die Registrierung beim externen Server ist fehlgeschlagen ... 11-9

Verbindungsprobleme mit Hosted Email Security ... 11-10

Bekannte Probleme mit dem Server ... 11-11
Inkonsistente Statussymbole ... 11-11
Spam-Daten inkonsistent mit Worry-Free Business Security Standard oder Advanced ... 11-11
Falscher Benutzername in der Worry-Free Business Security Services-Konsole ... 11-12
Inkonsistente Lizenzinfo in der Worry-Free Business Security Services-Konsole ... 11-12
Gleichzeitige Anmeldungen von zwei Registerkarten/Fenstern desselben Browsers sind nicht zulässig ... 11-12
Ältere Berichte werden automatisch gelöscht ... 11-13
Ein abgelaufenes Worry-Free Business Security Services-Konto kann nicht verwaltet werden ... 11-13
Unterbrochene ConnectWise-Verbindung ... 11-13

Bekannte Probleme mit dem Agent ... 11-14
Erneut installierte Agents liefern überlappende Daten ... 11-14
Ergebnisse des Befehls "Durchsuchen" können nicht überprüft werden ... 11-14
Agent-Konfigurationstool ist nach dem Upgrade des Agents nicht mehr sichtbar ... 11-14

Häufig gestellte Fragen 11-15
Häufig gestellte Fragen zur Webkonsole 11-15
Häufig gestellte Fragen zu Hosted Email Security 11-17
Häufig gestellte Fragen zu Berichten 11-18

Kapitel 12: Hilfe anfordern

Kontaktaufnahme mit Trend Micro 12-2
Problemlösung beschleunigen 12-2
Support-Portal verwenden 12-3
Enzyklopädie der Bedrohungen 12-3
Info über Trend Micro 12-4
TrendLabs 12-5

Stichwortverzeichnis

Stichwortverzeichnis IN-1

Vorwort

Vorwort

Das Remote Manager™-Benutzerhandbuch enthält Details zur Verwendung der Plattform sowie zur Ausführung grundlegender Aufgaben.

Zu den Themen gehören:

- *Info über Trend Micro auf Seite viii*
- *Zielpublikum auf Seite viii*
- *Textkonventionen auf Seite viii*

Info über Trend Micro

Als weltweit führender Anbieter für Cloud-Sicherheit entwickelt Trend Micro Lösungen für die Bereiche Internet-Content-Security und Bedrohungsverwaltung, die Schutzmaßnahmen für den Austausch digitaler Daten zwischen Unternehmen und Kunden bieten. Mit über 20 Jahren an Erfahrung zeichnet sich Trend Micro durch erstklassige Client-, Server- und cloudbasierte Lösungen aus, mit denen Sicherheitsbedrohungen schneller gestoppt und Daten in physischen, virtuellen und Cloud-Umgebungen geschützt werden können.

Beim Auftreten neuer Bedrohungen und Schwachstellen ist Trend Micro auch weiterhin entschlossen, Kunden dabei zu unterstützen, ihre Daten zu schützen, Compliance zu gewährleisten, Kosten zu reduzieren und die Integrität der Unternehmen zu sichern. Weitere Informationen finden Sie unter:

http://www.trendmicro.com

Trend Micro und das Trend Micro T-Ball-Logo sind Marken von Trend Micro Incorporated. In einigen Rechtsgebieten handelt es sich dabei um eingetragene Marken. Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken der entsprechenden Unternehmen.

Zielpublikum

Das Trend Micro Remote Manager Handbuch ist für Partner und Managed Service Providers (MSPs) vorgesehen, die die Plattform nutzen, um die gesamte Palette an Trend Micro SMB-Produkten all ihrer Kunden jederzeit und von jeder Stelle aus zu überwachen und zu verwalten.

Textkonventionen

Im Remote Manager™ Benutzerhandbuch werden die folgenden Konventionen verwendet.

TABELLE 1. Textkonventionen

KONVENTION	BESCHREIBUNG
NUR GROSSBUCHSTABEN	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Navigation > **pfad**	Navigationspfad für den Zugriff auf ein bestimmtes Fenster So bedeutet zum Beispiel **Datei** > **Speichern**: Klicken Sie in der Benutzeroberfläche auf **Datei** und dann auf **Speichern**.
Hinweis	Konfigurationshinweise
Tipp	Empfehlungen oder Anregungen
Warnung!	Kritische Aktionen und Konfigurationsoptionen

Kapitel 1

Einführung

Dieser Abschnitt enthält die folgenden Themen:

- *Trend Micro™ Remote Manager™ auf Seite 1-2*
- *Funktionen auf Seite 1-4*
- *Unterstützte Produkte auf Seite 1-9*
- *Neues auf Seite 1-22*
- *Globale Infrastruktur auf Seite 1-26*
- *Wichtige Begriffe auf Seite 1-28*

Trend Micro™ Remote Manager™

Trend Micro™Remote Manager™ ist eine leistungsstarke Konsole, die parallel mit der Trend MicroLicensing Management Platform™ zusammenarbeitet, um verwaltete Sicherheitsservices für mittelständische Unternehmen bereitzustellen.

Remote Manager ermöglicht die Überwachung der Integrität mehrerer verwalteter Netzwerke über verschiedene verwaltete Produkte und Services. Mit Trend Micro Remote Manager können Reseller-Administratoren Befehle erteilen, um kritische Aspekte der Netzwerksicherheit zu verwalten.

Remote Manager wird auf Servern in regionalen Trend Micro Datenzentren gehostet. Dort können Reseller ein eigenes Konto eröffnen. Mit Hilfe von Remote Manager können Reseller außerdem Kundenkonten einrichten, Kundennetzwerke überwachen sowie über die Remote Manager Web-Konsole die Sicherheit verwalten.

Remote Manager überwacht die folgenden Produkte:

- Worry-Free Business Security™ Standard (früher Client Server Suite) Versionen 6.x, 7.x, 8.x, 9.0
- Worry-Free Business Security Advanced (früher Client Server Messaging Suite) Versionen 6.x, 7.x, 8.x, 9.0
- Worry-Free Business Security Services Version 5.0, 5.1, 5.2, 5.3, 5.3 SP1, 5.6

Hinweis

Worry-Free Business Security Standard und Worry-Free Business Security Advanced sowie Worry-Free Business Security Services werden an den entsprechenden Stellen mit dem Sammelbegriff Worry-Free Business Security (alle) bezeichnet.

- Trend Micro Hosted Email Security™ Version 1.x
- Trend Micro Cloud Edge Version 2.8
- Trend Micro InterScan Web Security as a Service™ Version 2.0

Hinweis

Worry-Free Business Security Standard, Worry-Free Business Security Advanced, Worry-Free Business Security Services, Hosted Email Security, Cloud Edge und InterScan Web Security as a Service werden in diesem Dokument mit dem Sammelbegriff "verwaltete Produkte" und/oder "verwaltete Services" bezeichnet.

Remote Manager enthält ein Überwachungsdashboard, mit dem Reseller die folgenden Aspekte der Netzwerksicherheit überprüfen können:

- Worry-Free Business Security (alle):
  - Vorfälle in Zusammenhang mit Viren, Netzwerkviren und Spyware/Grayware
  - Vorfälle in Zusammenhang mit Spam und Phishing
  - Unbefugte Computermanipulationen
  - Ausbruchsituationen
  - Lizenz- und Update-Status von Sicherheitsprodukten
  - Speichernutzung auf Desktops, Servern und Exchange-Servern (nur Worry-Free Business Security Standard und Worry-Free Business Security Advanced)
  - Wichtige Sicherheitsindikatoren
- Hosted Email Security:
  - E-Mail-Verkehr
  - Größe der akzeptierten E-Mail-Nachrichten
  - Bedrohungsübersicht
  - Häufigste Empfänger von Spam
  - Häufigste Empfänger von Viren
- Cloud Edge
  - Gateways (Geräte) mit den meisten Bedrohungen
  - Kunden mit den meisten Bedrohungen

- InterScan Web Security as a Service:
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - URL-Filter
  - Anwendungskontrolle

Hinweis

Weitere Informationen über die oben genannten Produkte finden Sie in der jeweiligen Produktdokumentation unter: http://docs.trendmicro.com/de-de/home.aspx.

Remote Manager bietet eine strukturierte Ansicht der Kundennetzwerke und ermöglicht Resellern die Ausgabe von Befehlen sowie die Verwaltung der folgenden Aspekte der Netzwerksicherheit:

- Komponenten-Updates und Updates des verwalteten Servers
- Schwachstellenbewertung
- Schadensbeseitigung
- Automatische Ausbruchsreaktion
- Einstellungen der Firewall und Echtzeitsuche
- Manuelle Suche

Remote Manager unterstützt außerdem umfassende Berichtfunktionen; Reseller können für bestimmte Personen die automatische Erstellung von Berichten abonnieren.

Funktionen

Trend Micro Remote Manager bietet die folgenden Funktionen:

Integrierte Plattform

Remote Manager wird parallel zur Trend Micro™ Licensing Management Platform verwendet, mit einer zuverlässigeren Schnittstelle. Sie können über das Remote Manager Portal Folgendes ausführen:

- Neue Konten erstellen
- Lizenzen für einzelne Konten verlängern
- Weitere Arbeitsplätze hinzufügen

Remote Manager überwacht und verwaltet auch mehrere geschützte Netwerke über eine einzelne Konsole. Dies geschieht durch Kommunikation mit einem Remote Manager Agent, der auf den verwalteten Servern ausgeführt wird. Remote Manager ermöglicht außerdem die Ereignisüberwachung anhand wichtiger Sicherheitsindikatoren.

Dashboard-Widgets

Passen Sie die Widgets auf der Dashboard-Seite an. Mit Hilfe dieser Widgets werden Sie informiert, wenn Sie Lizenzen verlängern oder mehr zugeordnete Arbeitsplätze hinzufügen müssen oder bei welchen Kunden die meisten Bedrohungen auftreten.

Anpassbare Einstellungen für neue Konten

Bei der Erstellung neuer Konten können Sie die grundlegenden Standardeinstellungen anpassen, die standardmäßig von den neuen Konten verwendet werden sollen, oder die Einstellungen aus den Vorlagen auswählen, die Sie konfiguriert und gespeichert haben.

Bedrohungsstatus

Das Fenster "Ereignisse" von Remote Manager zeigt den Status der folgenden Aspekte der Netzwerksicherheit an:

- Worry-Free Business Security Standard und Worry-Free Business Security Advanced
    - Ausbruchsschutz

- Antivirus
- Anti-Spyware
- Web Reputation
- Verhaltensüberwachung
- Netzwerkviren
- Anti-Spam
- URL-Filter (nur Versionen 6.x und höher)
- Gerätesteuerung (nur Versionen 7.x, 8.x und 9.0)

- Worry-Free Business Security Services
  - Ausbruchsschutz
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - Verhaltensüberwachung
  - Netzwerkviren
  - URL-Filter
- Hosted Email Security
  - E-Mail-Verkehr gesamt
  - Größe der akzeptierten E-Mail-Nachrichten
  - Bedrohungsübersicht
  - Häufigste Empfänger von Spam
  - Häufigste Empfänger von Viren
- Cloud Edge
  - Botnet

    - Intrusion Prevention System (IPS)
    - Web Reputation
    - Virus
- InterScan Web Security as a Service:
    - Antivirus
    - Anti-Spyware
    - Web Reputation
    - URL-Filter
    - Anwendungskontrolle

Remote Manager bietet Details zu diesen Aspekten, darunter statistische Daten, wie die Anzahl von infizierten Computern und Viren-/Malware-Vorfällen. Reseller-Administratoren können darüber hinaus detaillierte Informationen, wie die Namen der betroffenen Computer oder der Bedrohungen, einsehen.

Systemstatus

Über das Fenster "Ereignisse" von Remote Manager können Reseller-Administratoren die folgenden systembezogenen Aspekte der Netzwerksicherheit überprüfen:

- Smart Protection Services
- Komponenten-Updates
- Wenig Festplattenspeicher
- Gerät/Agent ist offline
- Gerät/Agent ist offline (letzte 24 Stunden)
- Gerätestörung
- Gerätestörung (letzte 24 Stunden)
- AD/LDAP-Sync-Probleme

Lizenzstatus

Reseller-Administratoren können die folgenden lizenzbezogenen Details anzeigen:

- Erworbene Lizenzen (gesamt)
- Anzahl der genutzten Lizenzen
- Abgelaufene Lizenzen einschließlich Ablaufdatum
- Abgelaufene Lizenzen einschließlich Anzahl der Tage vor Ablauf der Lizenz

Netzwerkverwaltung

Remote Manager bietet eine strukturierte Ansicht der verwalteten Netzwerke und ermöglicht Reseller-Administratoren die Ausgabe von Befehlen und die Verwaltung der folgenden kritischen Aspekte der Netzwerksicherheit:

- Komponenten-Updates und Updates des verwalteten Servers
- Schwachstellenbewertung
- Automatische Ausbruchsreaktion
- Schadensbeseitigung
- Einstellungen der Firewall und Echtzeitsuche
- Manuelle Suche

Berichte

Neben Benachrichtigungen zu Sicherheitsereignissen kann Remote Manager automatisch regelmäßige Berichte erstellen und senden. Sie können Berichte nach Kunde, Produkt, Häufigkeit und Inhalt definieren und in verschiedenen Formaten abspeichern.

Integration in Tools von Drittanbietern

Aktivieren Sie die Protokollüberwachung mit Hilfe von Tools von Drittanbietern einschließlich Autotask™, Kaseya™ oder ConnectWise™, um die Aufgaben und Prozesse, die Sie überwachen, zu standardisieren.

Übermittlung von Feedback

Trend Micro möchte seinen Benutzern eine besonders gute und nützliche Plattform bereitstellen. Trend Micro hat jedoch keine Kenntnisse dahingehend, welche Services oder Funktionen Ihnen wichtig sind. Aus diesem Grund begrüßt Remote Manager Ihre Anmerkungen und Anregungen, die Sie über die Schaltfläche **Feedback übermitteln** mitteilen. Diese Schaltfläche wird im Banner angezeigt. Der Zugriff auf die Schaltfläche erfolgt ebenfalls über das Banner. Trend Micro kann diese Anmerkungen dann verarbeiten und ermitteln, welche Funktionen für die Mehrzahl der Benutzer hilfreich wären.

Unterstützte Produkte

- Worry-Free Business Security Standard
- Worry-Free Business Security Advanced
- Worry-Free Business Security Services
- Hosted Email Security
- Cloud Edge
- InterScan Web Security as a Service (IWSaaS)

Hinweis

Worry-Free Business Security Standard und Worry-Free Business Security Advanced sowie Worry-Free Business Security Services werden an den entsprechenden Stellen mit dem Sammelbegriff Worry-Free Business Security (alle) bezeichnet.

- Tools von Drittanbietern

- Autotask™
- Kaseya™
- ConnectWise™

Worry-Free Business Security Suite

Trend Micro™ Worry-Free Business Security Standard, Worry-Free Business Security Advanced und Worry-Free Business Security Services sind umfassende, zentral verwaltete Lösungen für kleine und mittlere Unternehmen.

Worry-Free Business Security Standard bietet Client-basierten Virenschutz und Firewall-Schutz für Desktop-Computer und Server. Worry-Free Business Security Advanced bietet neben den Funktionen von Worry-Free Business Security Standard eine Anti-Spam-Lösung zur Abwehr von E-Mail-Bedrohungen für Mail-Server, auf denen Microsoft™ Exchange Server ausgeführt wird. Worry-Free Business Security Standard und Worry-Free Business Security Advanced beinhalten eine Komponente auf dem Server zur Überwachung und Verwaltung des Client-Schutzes von einer zentralen Stelle aus.

Worry-Free Business Security Services bietet die meisten Vorteile von Worry-Free Business Security Standard. Weil Worry-Free Business Security Services außerdem ein gehosteter Service ist, können Sie die Sicherheitsfunktionen von jedem Ort aus zentral verwalten, ohne einen Server einrichten, installieren, konfigurieren oder warten zu müssen. Sicherheitsexperten von Trend Micro verwalten und aktualisieren den Service fortlaufend für Sie.

Hinweis

Weitere Informationen über Worry-Free Business Security Standard, Worry-Free Business Security Advanced und Worry-Free Business Security Services finden Sie in der Dokumentation unter:

http://docs.trendmicro.com/de-de/home.aspx

Trend Micro Remote Manager überwacht und verwaltet die durch Worry-Free Business Security Standard und Worry-Free Business Security Advanced geschützten Netzwerke, indem er mit einem Agent kommuniziert, der auf Worry-Free Business Security

Standard- und Worry-Free Business Security Advanced-Servern oder Worry-Free Business Security Services Servern in den Trend Micro Rechenzentren ausgeführt wird.

Hosted Email Security

Trend Micro™ Hosted Email Security sperrt Spam, Viren, Phishing und andere E-Mail-Bedrohungen, bevor sie Ihr Netzwerk erreichen. Eine gehostete Lösung erfordert weder Installation noch Wartung von Hard- oder Software und hilft Ihnen dabei, IT-Arbeitszeit und Benutzerproduktivität zurückzugewinnen. Sie verfügen wieder über mehr Bandbreite, mehr Speicherkapazität auf dem Mail-Server und eine höhere Prozessorleistung.

Außerdem verwaltet das weltweite Expertenteam von Trend Micro Hotfixes, Patches, Updates und Anwendungseinstellungen, um die Suchleistung kontinuierlich zu optimieren.

Hinweis

Weitere Informationen über Hosted Email Security finden Sie in der Dokumentation unter:

http://docs.trendmicro.com/de-de/home.aspx

Trend Micro Remote Manager Manager überwacht und verwaltet durch Hosted Email Security geschützte Netzwerke, indem er mit dem Hosted Email Security Server in den Trend Micro Rechenzentren kommuniziert.

Cloud Edge

In Cloud Edge sind die Vorteile einer Firewall der nächsten Generation vor Ort und die Annehmlichkeiten von Security-as-a-Service für Anbieter verwalteter Dienste vereint.

Cloud Edge stoppt Gefahren bereits am Gateway – durch intensives Scannen und Filtern von Netzwerkpaketen vor Ort oder in der Cloud. Cloud Edge kombiniert Anwendungskontrolle intelligent mit Benutzer- und Portidentifizierung, Zero-Day-Exploit-Erkennung, Suche nach Malware, Web Reputation-Sicherheit und URL-Filter und schützt damit Ihre Kunden vor Einbrüchen in ihr Netzwerk und Unterbrechung der Geschäftstätigkeit. Die Unterstützung von VPN sichert darüber hinaus

Verbindungen von Mobilgeräten, Unternehmens-Websites und Mitarbeitern, die unterwegs oder im Home Office arbeiten.

Implementieren Sie die Appliance Cloud Edge vor Ort ohne geografische Einschränkungen in Kundenbüros und kontrollieren Sie danach zentral Kundenzugriffe und Sicherheitsrichtlinien über eine intuitive Cloud-Konsole oder Trend Micro Remote Manager. Remote Manager arbeitet mit Cloud Edge durch Bereitstellung eines einzelnen Zugangspunkts für den Zugriff auf grafische Berichte und zusammengefasste Dashboard-Daten für unterstützte Appliances und Produkte von Trend Micro zusammen. Darüber hinaus können Sie mit Remote Manager die Lizenzvergabe an und die Rechnungsstellung für eine große Anzahl Kunden abwickeln.

InterScan Web Security as a Service

Einfach. Schnell. Kostengünstige Lösung.

Trend Micro versteht, wie wichtig der Schutz von Netzwerken ist und wie kostspielig die dafür benötigte technologische Infrastruktur sein kann. Daher haben wir mit unserer Expertise auf dem Gebiet der Cloud-Technologie ein elastisches Gateway-Produkt für Cloud-Sicherheit geschaffen – InterScan Web Security as a Service (IWSaaS).

Da es sich hierbei um eine Cloud-basierte Anwendung handelt, muss weder in Hardware noch Software investiert werden. Mit Hilfe von IWSaaS können Sie sich auf die strategische Sicherheit, wie Richtlinien und Architektur, konzentrieren, statt sich mit den operativen Aufgaben zur Verwaltung der Netzwerkinfrastruktur zu beschäftigen.

Unsere Cloud-Lösung bietet Ihnen:

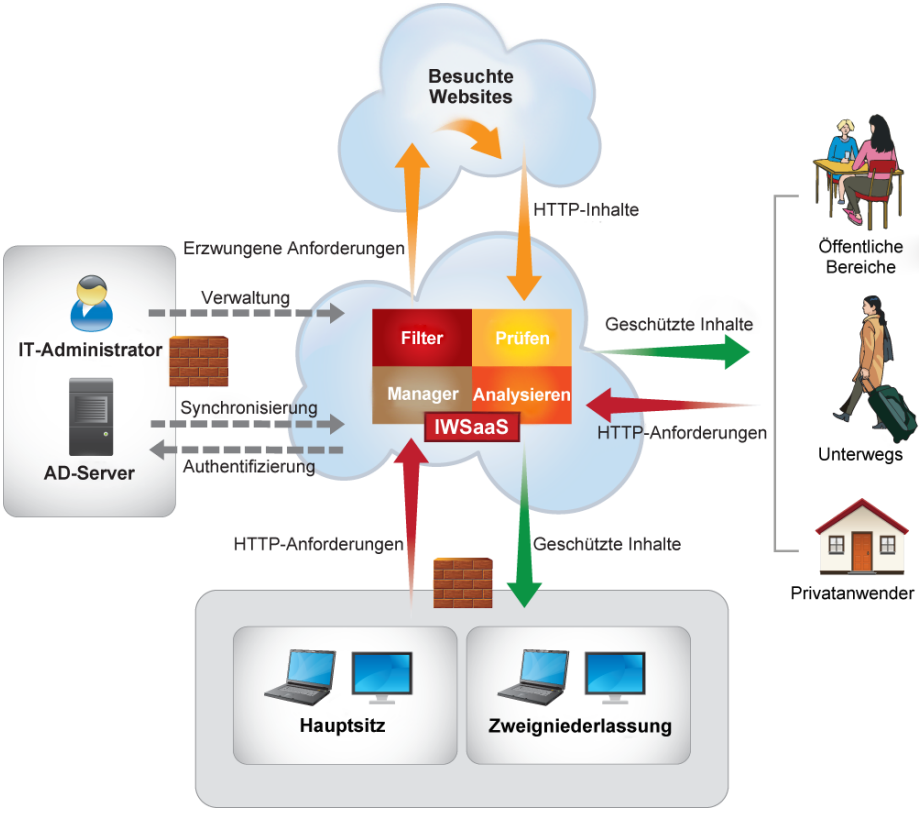
- Schutz vor Viren und anderen Sicherheitsrisiken in Datei-Uploads und -Downloads mit flexibel konfigurierbarer Anti-Malware-Schutztechnologie. Darüber hinaus sucht IWSaaS nach zahlreichen Arten von Spyware, Grayware und anderen Risiken.
- Sperre von Websites, die vom Web-Reputation-Dienst (WRS) als bösartig eingestuft wurden, basierend auf dem Reputationswert einer Website.
- Kontrolle von Internetanwendungen, die von der Anwendungskontrolle anhand von Richtlinien entdeckt wurden.
- Steuerung des Zugriffs auf bestimmte Websites mit Hilfe von Listen für zulässige/gesperrte Websites.

- Durchsuchen des Datenverkehrs nach URL-Kategorien, wie „Für Erwachsene“ und „Glücksspiel“. Wenn ein Benutzer eine URL anfordert, schlägt IWSaaS unter Verwendung von URL-Filterrichtlinien zunächst die Kategorie für diese URL nach und ermöglicht, verweigert oder überwacht dann den Zugriff basierend auf den festgelegten Richtlinien.
- Überwachung und Analyse des Webverkehr-Status mit Hilfe der Bericht- und Protokollabfrage-Funktion des Dashboards.

So funktioniert IWSaaS

Das Diagramm unten veranschaulicht, wie IWSaaS den Netzwerkverkehr in der Cloud verwaltet. Wenn ein Benutzer eine **HTTP**-Anforderung sendet, entweder innerhalb oder außerhalb der Firewall, wird der Datenverkehr dieses Benutzers durch die Cloud geleitet. IWSaaS prüft die Anforderung, analysiert sie und filtert sie basierend auf den von den Administratoren festgelegten Richtlinien. Wenn die Anforderung zulässig ist und der Benutzer sich bei IWSaaS anmeldet, sendet IWSaaS den sicheren Inhalt zurück an den Benutzer. Wenn die Anforderung nicht zulässig ist, beispielsweise eine

Anforderung einer verbotenen URL-Kategorie, blockiert IWSaaS die Anforderung und benachrichtigt den Benutzer.



Durch Klicken auf die Schaltfläche mit dem blauen Fragezeichen auf einer beliebigen Seite können Sie die Hilfe für diese Seite öffnen. Die seitenbezogene Hilfe wird in einem Fenster angezeigt. In diesem Fenster werden Informationen, die zur Fertigstellung des Bildschirms benötigt werden, auf der Registerkarte "Schritte" sowie zusätzliche Informationen zu dem Vorgang auf der Registerkarte "Mehr" aufgeführt.

Sie können die inhaltsbezogene Hilfe aufrufen. Diese umfasst die Hilfetexte aus dem Hilfemenü im Hauptbanner zusammen mit der Readme-Datei, der Anleitung zu den ersten Schritten und der Kurzanleitung.

Tools von Drittanbietern

Trend Micro Remote Manager kann in Tools von Drittanbietern integriert werden, um eine sicherere Netzwerkumgebung zu gewährleisten. Tools hierfür sind:

Autotask™

Remote Manager kann die folgenden Ereignisbenachrichtigungen an das Autotask-System senden:

- Worry-Free Business Security Standard und Worry-Free Business Security Advanced
    - Agent ungewöhnlich
    - Ausbruchsschutz
    - Antivirus
    - Anti-Spyware
    - Web Reputation
    - Verhaltensüberwachung
    - Netzwerkvirus
    - Anti-Spam
    - Nicht mehr aktuelle verwaltete Server
    - Ungewöhnliche Systemereignisse
    - Lizenzablauf
    - URL-Filter
    - Gerätesteuerung

    - Herunterfahren von Worry-Free Business Security Standard und Worry-Free Business Security Advanced Server
    - Herunterfahren von Exchange Server
    - Probleme mit Active Directory-Synchronisierung
- Worry-Free Business Security Services
    - Agent ungewöhnlich
    - Ausbruchsschutz
    - Antivirus
    - Anti-Spyware
    - Web Reputation
    - Verhaltensüberwachung
    - Netzwerkvirus
    - Nicht mehr aktuelle verwaltete Server
    - Ungewöhnliche Systemereignisse
    - Lizenzablauf
    - URL-Filter
    - Herunterfahren von Exchange Server
    - Probleme mit Active Directory-Synchronisierung
- Hosted Email Security
    - E-Mail-Verkehr gesamt
    - Größe der akzeptierten E-Mail-Nachrichten
    - Bedrohungsübersicht
    - Häufigste Empfänger von Spam
    - Häufigste Empfänger von Viren

- Cloud Edge
  - Botnet
  - Intrusion Prevention System (IPS)
  - Web Reputation
  - Virus
- InterScan Web Security as a Service:
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - URL-Filter
  - Anwendungskontrolle

Diese Ereignisse werden in Form von E-Mail-Nachrichten an Autotask gesendet, wo sie in Autotask-Tickets umgewandelt werden. Damit dies geschieht, müssen Benachrichtigungsempfänger zur Remote Manager Web-Konsole hinzugefügt und mehrere Felder im Autotask-Ticketsystem erstellt werden. Weitere Informationen finden Sie unter *Integration von Autotask™ auf Seite 4-16*.

Kaseya™

Remote Manager und Worry-Free Business Security Services können Ereignisbenachrichtigungen an das Kaseya-System senden. Die folgenden Ereignisse können an Kaseya gesendet werden:

- Worry-Free Business Security Standard und Worry-Free Business Security Advanced
  - Agent ungewöhnlich
  - Ausbruchsschutz
  - Antivirus
  - Anti-Spyware

- Web Reputation
- Verhaltensüberwachung
- Netzwerkvirus
- Anti-Spam
- Nicht mehr aktuelle verwaltete Server
- Ungewöhnliche Systemereignisse
- Lizenzablauf
- URL-Filter
- Gerätesteuerung
- Herunterfahren von Client Server Messaging/Worry-Free Business Security Standard und Worry-Free Business Security Advanced Server
- Herunterfahren von Exchange Server

- Worry-Free Business Security Services
  - Agent ungewöhnlich
  - Ausbruchsschutz
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - Verhaltensüberwachung
  - Netzwerkvirus
  - Nicht mehr aktuelle verwaltete Server
  - Ungewöhnliche Systemereignisse
  - Lizenzablauf
  - URL-Filter

    - Herunterfahren von Exchange Server
- Hosted Email Security
    - E-Mail-Verkehr gesamt
    - Größe der akzeptierten E-Mail-Nachrichten
    - Bedrohungsübersicht
    - Häufigste Empfänger von Spam
    - Häufigste Empfänger von Viren
- Cloud Edge
    - Botnet
    - Intrusion Prevention System (IPS)
    - Web Reputation
    - Virus
- InterScan Web Security as a Service:
    - Antivirus
    - Anti-Spyware
    - Web Reputation
    - URL-Filter
    - Anwendungskontrolle

Diese Ereignisse werden in Form von E-Mail-Nachrichten an Kaseya gesendet, wo sie in Kaseya-Tickets umgewandelt werden. Damit dies geschieht, müssen Benachrichtigungsempfänger zur Remote Manager Web-Konsole hinzugefügt und mehrere Felder im Kaseya-Ticketsystem erstellt werden. Weitere Informationen finden Sie unter *Integration von Kaseya™ auf Seite 4-23*.

Worry-Free Business Security Services-Bereitstellungstool für Kaseya

Kaseya bietet ein Tool zur stapelweisen Bereitstellung von Worry-Free Business Security Services-Clients über die Kaseya-Konsole. Laden Sie das Tool auf dieser Seite herunter und verwenden Sie es hier, um fortzufahren.

Hinweis

Dies ist ein Tool von einem Drittanbieter, das zur Unterstützung bei der Produktintegration bereitgestellt wird, es ist jedoch kein Produkt von Trend Micro.

ConnectWise™

Remote Manager und Worry-Free Business Security Services können Ereignisbenachrichtigungen an das ConnectWise-System senden. Die folgenden Ereignisse können an ConnectWise gesendet werden:

- Worry-Free Business Security Standard und Worry-Free Business Security Advanced
  - Agent ungewöhnlich
  - Ausbruchsschutz
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - Verhaltensüberwachung
  - Netzwerkvirus
  - Anti-Spam
  - Nicht mehr aktuelle verwaltete Server
  - Ungewöhnliche Systemereignisse
  - Lizenzablauf

    - URL-Filter
    - Gerätesteuerung
    - Herunterfahren von Client Server Messaging/Worry-Free Business Security Standard und Worry-Free Business Security Advanced Server
    - Herunterfahren von Exchange Server
- Worry-Free Business Security Services
    - Agent ungewöhnlich
    - Ausbruchsschutz
    - Antivirus
    - Anti-Spyware
    - Web Reputation
    - Verhaltensüberwachung
    - Netzwerkvirus
    - Nicht mehr aktuelle verwaltete Server
    - Ungewöhnliche Systemereignisse
    - Lizenzablauf
    - URL-Filter
    - Herunterfahren von Exchange Server
- Hosted Email Security
    - E-Mail-Verkehr gesamt
    - Größe der akzeptierten E-Mail-Nachrichten
    - Bedrohungsübersicht
    - Häufigste Empfänger von Spam
    - Häufigste Empfänger von Viren

- Cloud Edge
  - Botnet
  - Intrusion Prevention System (IPS)
  - Web Reputation
  - Virus
- InterScan Web Security as a Service:
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - URL-Filter
  - Anwendungskontrolle

Diese Ereignisse werden in Form von E-Mail-Nachrichten an ConnectWise gesendet, wo sie in ConnectWise protokolliert werden. Damit dies geschieht, müssen Benachrichtigungsempfänger zur Remote Manager Web-Konsole hinzugefügt und mehrere Felder im ConnectWise Ticketsystem erstellt werden. Weitere Informationen finden Sie unter *Integration von ConnectWise™ auf Seite 4-30*.

Neues

Trend Micro™ Remote Manager umfasst die folgenden neuen Funktionen und Erweiterungen:

TABELLE 1-1. Neu in der Version von Dezember 2014

MERKMAL	BESCHREIBUNG
InterScan Web Security as a Service (IWSaaS)-Integration	Trend Micro Remote Manager arbeitet mit IWSaaS, indem ein einzelner Zugangspunkts für den Zugriff auf grafische Berichte und zusammengefasste Dashboard-Daten für IWSaaS bereitgestellt wird. Sie können auch auf der Seite "Kunden" auf den Link **Konsole öffnen** klicken, um die Web-Konsole zu öffnen:

Verbesserungen bei Widgets	• Neues IWSaaS-Widget bereitgestellt.
	• IWSaaS-Daten zu folgenden Widgets hinzugefügt:
	  • Bedrohungsverwaltung
	  • Systemverwaltung
	  • Verwaltete Kunden und Produkte/Services
	  • Lizenzverwaltung
	  • Nutzung von Test- und Volllizenzen
	  • Kunden, die besonderer Aufmerksamkeit bedürfen
	• Die Widget-Schaltflächen verbessert, indem mit Hilfe eines Dropdown-Menüs der Platz für die Widget-Namen vergrößert wurde.

TABELLE 1-2. Neu in der Version von Juli 2014

MERKMAL	BESCHREIBUNG
Integration von Cloud Edge	Trend Micro Remote Manager arbeitet mit Cloud Edge durch Bereitstellung eines einzelnen Zugangspunkts für den Zugriff auf grafische Berichte und zusammengefasste Dashboard-Daten für Cloud Edge-Appliances zusammen. Darüber hinaus können Sie mit Trend Micro Remote Manager die Lizenzvergabe an und die Rechnungsstellung für Cloud Edge-Kunden abwickeln.
Agent-Version	Sie können nun die Version von Worry-Free Business Security Services Agent auf der Produktkonsole sehen.
Berichte	Verbesserte Anzeige der durch Umwandlung von HTML- in PDF-Format erzeugten Dateien.
Verbesserungen bei Widgets	• Neue Funktionen und Verbesserungen/ Ergänzungen. • Beseitigung von Leistungsproblemen. • Beseitigung von Problemen durch Überlagerung.

TABELLE 1-3. Neu in der Version von Juni 2014

FUNKTION/ERWEITERUNG	DETAILS
Aktionsfähige Benachrichtigung	Unter den in den Widgets oder in der E-Mail-Benachrichtigung aufgeführten Links werden Ihnen die Lizenzen angezeigt, bei denen sofort oder demnächst Handlungsbedarf besteht. Durch Klicken auf die Ereignisse kann auch die Web-Konsole bestimmter Produkte geöffnet werden. Weitere Informationen finden Sie unter "Single-Sign-On".
Berichte anpassen	Partner und Kunden haben hinsichtlich der Berichte, die sie empfangen, unterschiedliche Anforderungen. Durch Verwendung der neuen Inhalte und Berichte können Sie sicherstellen, dass die Benutzer die richtigen Informationen erhalten.

Funktion/Erweiterung	Details
Neue Kunden in drei einfachen Schritten einrichten **Hinweis** Diese Funktion steht nur Benutzern der Trend Micro Licensing Management Platform zur Verfügung. Weitere Informationen erhalten Sie bei Ihrem Managed Service Provider oder bei einem Vertreter von Trend Micro.	Die Standardrichtlinien für neue Kunden können Sie in drei (3) Schritten einrichten und bereitstellen. Dadurch erhalten diese Kunden das gleiche Niveau an Schutz und Überwachung durch den Trend Micro Remote Manager.
Standardeinstellungsvorlagen anpassen **Hinweis** Diese Funktion steht nur Benutzern der Trend Micro Licensing Management Platform zur Verfügung. Weitere Informationen erhalten Sie bei Ihrem Managed Service Provider oder bei einem Vertreter von Trend Micro.	Konfigurieren Sie vorab unterschiedliche Vorlagen für die Einstellungen für Worry-Free Business Security Services. Dann können Sie für Ihre Kunden verschiedene Dienstmodelle flexibel anpassen.
Single-Sign-On	Klicken Sie auf der Seite "Kunden" auf den Link **Konsole öffnen**, um die Web-Konsole der folgenden Services zu öffnen: • Worry-Free Business Security Services • Hosted Email Security • Cloud Edge

FUNKTION/ERWEITERUNG	DETAILS
Weitere Hilfe	In Trend Micro Remote Manager kann einfach über die Schaltfläche **Hilfe** auf die Dokumentation zugegriffen werden. Diese enthält auch Video-Tutorials, die direkt in der Konsole angesehen werden können. Trend Micro Remote Manager enthält auch einen Link zum Trend Micro Remote Manager Leitfaden mit bewährten Methoden.

Globale Infrastruktur

Trend Micro Remote Manager besteht aus drei Grundkomponenten:

- Reseller
- Trend Micro Rechenzentrum
- Kundennetzwerk

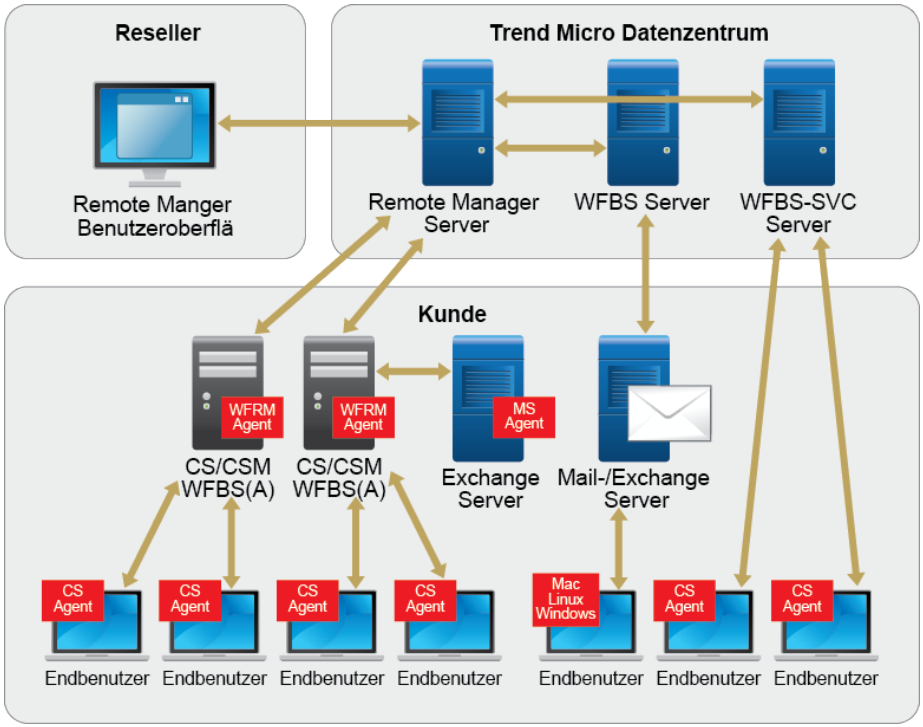


ABBILDUNG 1-1. Remote Manager – Globale Architektur

Der Reseller greift über die Remote Manager Web-Konsole per Internet auf ein Trend Micro-Datenzentrum zu. Bisher sind Datenzentren auf vier Kontinenten eingerichtet. Der Reseller muss keine Installation ausführen, um das Produkt verwenden zu können. Der Reseller muss jeden Kunden in der Remote Manager Web-Konsole hinzufügen und konfigurieren, bevor der Reseller die Kundenkonten verwalten kann.

Auf jedem über Worry-Free Business Security Standard und Advanced verwalteten Server ist ein Remote Manager Agent installiert, der die Kommunikation mit den Remote Manager Servern ermöglicht. Da die Worry-Free Business Security Services im Trend Micro Rechenzentrum gehostet werden, muss kein Agent installiert werden. Worry-Free Business Security Services muss jedoch für jeden Kunden an der Remote Manager Web-Konsole registriert werden.

Der Remote Manager Agent, der über die Remote Manager Web-Konsole installiert werden kann, wird auf dem über Worry-Free Business Security Standard und Advanced verwalteten Server im Kundennetzwerk ausgeführt. Der Remote Manager Agent sendet Informationen an den Remote Manager Server, über den Sie die Daten mit einer Internet-Verbindung rund um die Uhr auf Ihrer Konsole abrufen können.

Wichtige Begriffe

Die folgenden Begriffserläuterungen sollen ein effizienteres Arbeiten mit Remote Manager ermöglichen:

BEGRIFF	DEFINITION
Agent	Dieses Programm wird auf Worry-Free Business Security Standard und Advanced Servern installiert und ermöglicht Remote Manager die Überwachung und Verwaltung von Worry-Free Business Security Standard und Advanced.
Bewertung	Regelmäßige Überprüfungen der Daten aus Kundennetzwerken zur Ermittlung der Integrität der überwachten Netzwerke. Bei diesen Überprüfungen werden wichtige Indikatoren verwendet, die so genannten Bewertungsindizes.
Bewertungsindizes	Die Grundlage für Sicherheitsbewertungen; Reseller-Administratoren können die einzelnen Indizes anpassen, um die Bewertungsintervalle, Bereiche und Benachrichtigungen festzulegen.
Client Security Agent (CSA)	Der Agent, der an den Worry-Free Business Security Server berichtet. Der CSA sendet Ereignisstatusinformationen in Echtzeit. Agents berichten beispielsweise über Ereignisse, wie entdeckte Bedrohungen, das Starten und Herunterfahren des Agents, den Startzeitpunkt einer Suche oder einen abgeschlossenen Update-Vorgang. Der CSA stellt drei Suchmethoden zur Verfügung: die Echtzeitsuche, die zeitgesteuerte Suche und die manuelle Suche. Sie können die Sucheinstellungen für die Agents auf der Webkonsole konfigurieren.

BEGRIFF	DEFINITION
Dashboard	Das Dashboard in Remote Manager ist das Hauptfenster (Registerkarte **Home**), in dem die Web-Konsole und die Widgets angezeigt werden.
Erkennung	Das Entdecken einer Bedrohung; ein Fund deutet nicht auf eine Systeminfektion hin, sondern nur darauf, dass Malware den Computer erreicht hat. Wird dieselbe Bedrohung auf mehreren Computern entdeckt, kann dies auf einen Ausbruch hindeuten.
Ereignis	Das Auftreten eines Zustands in einer überwachten Domäne.
GUID (Globally Unique Identifier) oder Autorisierungsschlüssel	Eine eindeutige Referenznummer, die als ID in Computersoftware verwendet wird.
Infektion	Die Bedingung, bei der eine Bedrohung ihre Schadteile auf einem Computer ausführen kann; Remote Manager geht immer dann vom Auftreten einer Infektion aus, wenn der Virenscanner einen Virus oder eine Malware erkennt und die Bedrohung nicht säubern, löschen oder in Quarantäne verschieben kann. Eine Spyware-/Grayware-Infektion tritt dann auf, wenn der Computer nur durch einen Neustart komplett gesäubert werden kann.
Messaging Security Agent (MSA)	Der Agent, der sich auf Microsoft Exchange Servern befindet und an Client Server Messaging und Worry-Free Business Security Advanced Server berichtet. Dieser Agent bietet Schutz vor Viren und Malware, Trojanern, Würmern und anderen Bedrohungen in E-Mails. Außerdem umfasst er Spam-Schutz, Content-Filter und das Sperren von Anhängen.
Reseller	Allgemeiner Begriff, der Unternehmen bezeichnet, die Dienste zur Sicherheitsüberwachung und -verwaltung für Kunden in Remote Manager bereitstellen.
Reseller-Administratoren	Administratoren auf Seite des Resellers, die mit Hilfe von Remote Manager Dienstleistungen bereitstellen.
Trend Micro Datenzentrum	Das Überwachungs- und Verwaltungszentrum von Trend Micro, in dem Remote Manager (und Hosted Email Security) Server gehostet werden und Support für Reseller-Administratoren bereitgestellt wird.

BEGRIFF	DEFINITION
Security Server	Der Worry-Free Business Security Standard und Worry-Free Business Security Advanced Servercomputer.
Virenwarnung	Ein Aufruf zur Wachsamkeit von TrendLabs℠, um Kundennetzwerke für einen Virenausbruch zu rüsten; TrendLabs sendet Warnungen an verschiedene Trend Micro Produkte und liefert vorbeugende Lösungen, die IT-Administratoren als erste Verteidigungslinie implementieren können, bevor ein Pattern erhältlich ist.
Virenausbruch	Die schnelle Verbreitung einer Virenbedrohung auf verschiedene Computer und Netzwerke; je nach Verbreitung der Bedrohung kann ein Ausbruch intern, regional oder global sein.

Kapitel 2

Erste Schritte

Dieser Abschnitt enthält die folgenden Themen:

- *Browser-Anforderungen auf Seite 2-2*
- *Auf die Plattform zugreifen auf Seite 2-3*
- *Koordination mit dem Kunden auf Seite 2-4*

Browser-Anforderungen

- Internet-Verbindung
- Remote Manager Kontoinformationen von Trend Micro
- Unterstützte Browser:
  - Neueste Firefox™-Version (empfohlen)
  - Neueste Version von Google™ Chrome™ (empfohlen)
  - Internet Explorer™ 9.0

URL der Trend Micro Remote Manager Web-Konsole zu den vertrauenswürdigen Sites hinzufügen

Fügen Sie die Remote Manager Web-Konsolen-URL zur Liste der vertrauenswürdigen Sites in Internet Explorer hinzu, um problemlos auf alle Konsolenfenster und -funktionen zugreifen zu können.

Prozedur

1. Öffnen Sie Internet Explorer.
2. Klicken Sie auf die Registerkarte **Extras** > **Internetoptionen** > **Sicherheit**.
3. Wählen Sie die Zone **Vertrauenswürdige Sites**.
4. Klicken Sie auf **Websites...**.
5. Geben Sie unter **Diese Website zur Zone hinzufügen** den Konsolen-URL ein.
6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **OK**.

SSL-Zertifikat mit Internet Explorer 9 ermitteln

Um den Agent zu verwenden, fügen Sie dem Browser das SSL-Zertifikat von Trend Micro auf dem verwalteten Server hinzu.

Prozedur

1. Öffnen Sie Internet Explorer und wechseln Sie (je nach Region) zur Website Trend Micro Remote Manager.
2. Doppelklicken Sie auf das Vorhängeschloss-Symbol rechts von der Adressleiste.

   Die Websiteidentifizierung wird angezeigt.
3. Klicken Sie auf **Zertifikate anzeigen**.

   Das Fenster "Zertifikat" mit dem für `*.trendmicro.com` ausgestellten Zertifikat wird geöffnet.
4. Navigieren Sie zu **Zertifizierungspfad (Registerkarte)** > **GeoTrust oder Zertifizierungsstelle Equifax Secure** > **Zertifikat anzeigen**.
5. Klicken Sie im Fenster **Zertifikat**, in dem die Zertifikatsinformationen angezeigt werden, auf die Registerkarte **Details**.
6. Wechseln Sie zu **In Datei kopieren** > **Weiter** und wählen Sie anschließend **DER-kodiert-binär X.509 (.CER)**.
7. Klicken Sie auf **Weiter**, und geben Sie dann den Pfad und Dateinamen des Zertifikats ein.

   Zum Beispiel: `wfrmcert.cer`.
8. Klicken Sie auf **Weiter** > **Fertig stellen**.

Auf die Plattform zugreifen

Alle Benutzer melden sich, unabhängig vom Kontotyp und den Berechtigungen, auf derselben Seite an. Geben Sie Ihre Anmeldeinformationen ein und klicken Sie auf

Anmelden. Sie sollten Ihre Anmelde-URL und Ihre Anmeldeinformationen von dem Benutzer mit dem übergeordneten Konto erhalten.

Benutzer können keine Einstellungen oder Optionen anzeigen, für die sie keine Anzeigeberechtigungen haben.

Koordination mit dem Kunden

Die Überwachung und Verwaltung des Netzwerks Ihres Kunden durch Trend Micro Remote Manager bietet zahlreiche Vorteile für Ihren Kunden. Wie bei allen anderen Aktivitäten der Remote-Verwaltung können Eingriffe über die Konsole jedoch drastische Auswirkungen auf das verwaltete Netzwerk haben.

Vor der Service-Bereitstellung sollten Sie die Zustimmung des Kunden einholen, um die folgenden Aktivitäten zur Remote-Verwaltung und -Überwachung durchzuführen:

- Anzeige der Liste aller Computer im Kundennetzwerk
- Verlängerung der Lizenzen oder Hinzufügen neuer Arbeitsplatzlizenzen
- Anzeige der folgenden Sicherheitsinformationen:
    - Entdeckte Viren/Malware, Spyware/Grayware und Netzwerkviren
    - Namen und Anzahl infizierter Computer
    - Namen infizierter Dateien
    - E-Mail-Adressen, die infizierte Dateien empfangen haben
    - Patch-Informationen über bekannte Sicherheitslücken
    - Lizenz- und Systeminformationen über Worry-Free Business Security (alle) und Hosted Email Security
- Senden von Benachrichtigungen an Personen im Unternehmen des Kunden
- Durchführung der folgenden Maßnahmen:
    - Sicherheitskomponenten verteilen
    - Suchläufe zur Schwachstellenbewertung starten

- Damage Cleanup Services starten
- Manuelle Suchläufe starten oder beenden
- Aktualisieren der Worry-Free Business Security Standard und Worry-Free Business Security Advanced Server
- Starten oder Beenden des Ausbruchsschutzes

- Konfigurieren Sie die folgenden Einstellungen:
  - Automatische Verteilung des Ausbruchsschutzes
  - Echtzeitsuche
  - Firewall
  - Location Awareness
  - Verhaltensüberwachung
  - Web Reputation
  - URL-Filter
  - Gerätesteuerung (Worry-Free Business Security 7.0 und höher)

Kapitel 3

Die Web-Konsole verstehen

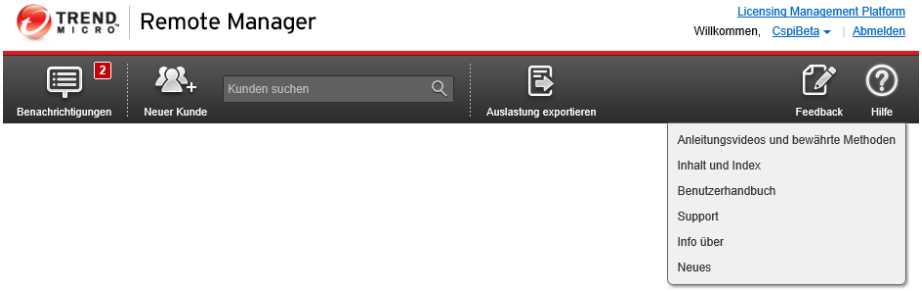
Die Web-Konsole ist die zentrale Stelle zur Überwachung und Verwaltung von Produkten und Kunden.

Dieser Abschnitt enthält die folgenden Themen:

- *Das Web-Konsolen-Banner auf Seite 3-2*
- *Hauptmenü auf Seite 3-5*
- *Das Dashboard verstehen auf Seite 3-7*

Das Web-Konsolen-Banner

Der Bannerbereich bietet die folgenden Optionen:

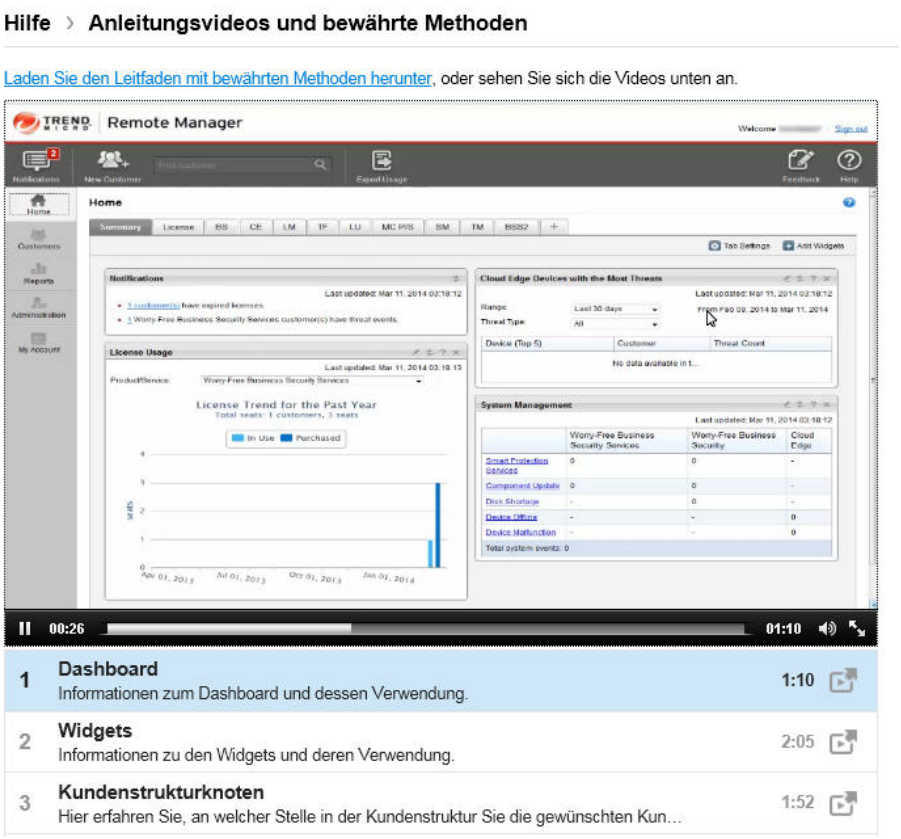


- **<Kontoname>**: Zeigt das derzeit angemeldete Konto an.
- **Abmelden**: Meldet Sie aus der Web-Konsole ab.
- **Licensing Management Platform**: Dieser Link wird nicht angezeigt, wenn Sie diesen in die License Management Platform-Website integriert haben.
- **Benachrichtigungen**: Zeigt an, für wie viele Ereignisse Aktionen erforderlich sind.
- **Neuer Kunde**: Klicken Sie auf diese Schaltfläche, um einen neuen Kunden hinzuzufügen.
- **Suchleiste**: Geben Sie Kundeninformationen an, um einen spezifischen Kunden schnell auffinden zu können.
- **Auslastung exportieren**: Klicken Sie auf diese Schaltfläche, um ein Dokument zu exportieren, in dem Ihre genutzten Lizenzen angegeben sind.
- **Feedback**: Klicken Sie auf diese Schaltfläche, um wertvolles Feedback an Trend Micro zu senden in Bezug auf Ihre Verwendung des Produkts und welche Funktionen aus Ihrer Sicht ergänzt werden sollten oder wie aktuelle Funktionen noch verbessert werden können.
- **Hilfe**:

- **Anleitungsvideos und bewährte Methoden**: Es wird eine Seite geöffnet, auf der Sie die Anleitungsvideos ansehen können und auf der Sie einen Link zu bewährte Methoden finden.
- **Inhalt und Index**: Öffnet die Trend Micro Remote Manager Online-Hilfe.
- **Benutzerhandbuch**: Das Benutzerhandbuch kann heruntergeladen oder im PDF-Format angezeigt werden.
- **Support**: Zeigt die Trend Micro Webseite "Support" an, auf der Sie eine Anfrage an das Support-Team von Trend Micro stellen können und Antworten auf häufig gestellte Fragen zu den Produkten von Trend Micro finden.
- **Info**: Gibt einen Überblick zum Produkt an und enthält Anweisungen zur Überprüfung der Versionsdetails der Komponenten.
- **Neues**: Verknüpfung zu der Seite, auf der Sie über die neuen Funktionen informiert werden.

Anleitungsvideos und bewährte Methoden

Auf dieser Seite können Sie Folgendes herunterladen bzw. ansehen:

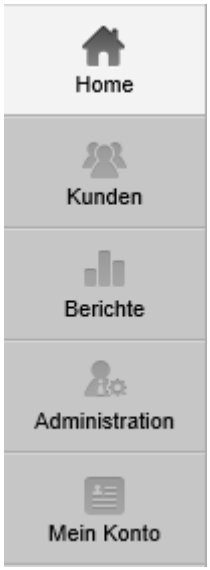

Hilfe › Anleitungsvideos und bewährte Methoden
Laden Sie den Leitfaden mit bewährten Methoden herunter, oder sehen Sie sich die Videos unten an.
Remote Manager
00:26
01:10
1 Dashboard
Informationen zum Dashboard und dessen Verwendung.
1:10
2 Widgets
Informationen zu den Widgets und deren Verwendung.
2:05
3 Kundenstrukturknoten
Hier erfahren Sie, an welcher Stelle in der Kundenstruktur Sie die gewünschten Kun…
1:52

- Leitfaden mit bewährten Methoden: Der technische Support von Trend Micro hat einen Leitfaden mit bewährten Methoden bereitgestellt, der Sie bei der Vorbereitung und Einrichtung Ihrer Infrastruktur unterstützen soll.

- Anleitungsvideos: Auf dieser Seite können Sie vom technischen Support von Trend Micro erstellte Videos zu einer Vielzahl von Artikeln ansehen, die das jeweilige Produkt oder dessen Verwendung detailliert veranschaulichen.

Hauptmenü

Im Hauptmenü werden die Schaltflächen angezeigt, über die Sie zu Funktionen und Optionen navigieren können. Über die Navigationsleiste können Sie auf folgende Elemente klicken:

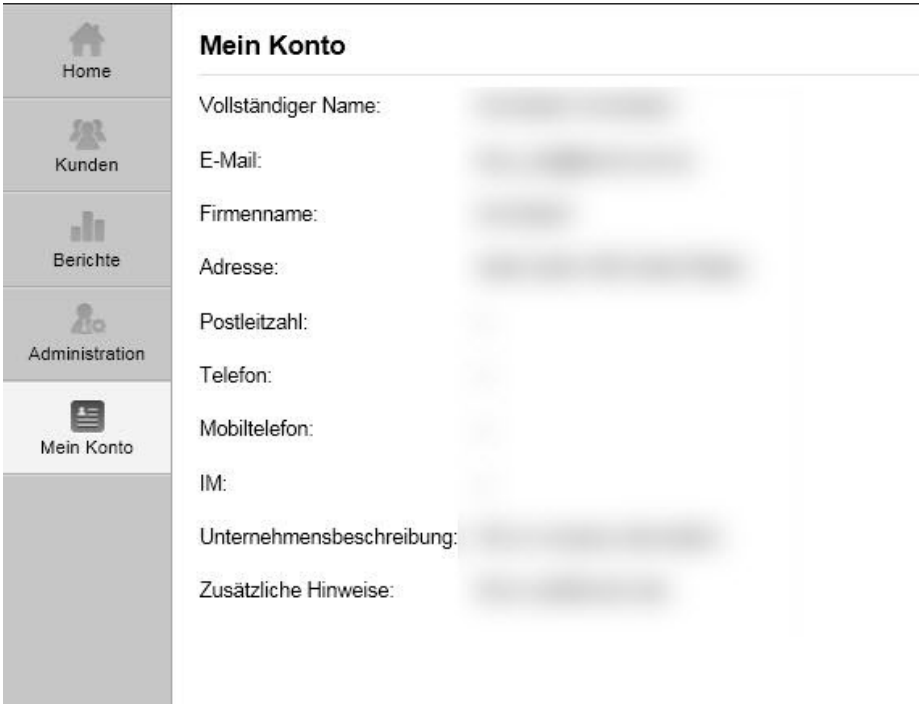


- **Home**: Sie werden zur Startseite geleitet, auf der das Dashboard und im rechten Bereich die Widgets angezeigt werden.
- **Kunden**: Zeigt die Liste der Kunden an, in der Sie Kunden hinzufügen können oder Änderungen an den Kundeneinstellungen oder -konfigurationen vornehmen können.
- **Berichte**: Zeigt die Berichte an sowie die neuen Berichte, die hinzugefügt werden können.

- **Administration**: Auf dieser Seite können Sie die Einstellungen für Benachrichtigungen oder die Web-Konsole und die Standardeinstellungsvorlagen ändern oder die Integration mit Tools anderer Anbieter konfigurieren.
- **Mein Konto**: Wird nur angezeigt, wenn Ihr Konto nicht in die Licensing Management Platform integriert ist.

Mein Konto

Auf dieser Seite werden Ihre Kontoeinstellungen angezeigt. Die Seite erscheint jedoch nur, wenn Sie Ihr Konto nicht mit der Licensing Management Platform integriert haben.



Das Dashboard verstehen

Dieser Abschnitt enthält Informationen zu Registerkarten, Widgets und dem Dashboard.

Dashboard Statusfenster

Das Dashboard ist das zentrale Fenster zur Überprüfung des Status überwachter Netzwerke. Das Dashboard zeigt nur Produkte mit ungewöhnlichem Status. Wenn z. B. die Worry-Free Business Security Services Lizenz eines Kunden abläuft oder ein Kunde zu viele Bedrohungen aufweist, werden diese Kunden hier aufgeführt.

Öffnen Sie einen kompatiblen Browser und melden Sie sich auf der Seite Trend Micro Remote Manager für Ihre Region an, um auf das Dashboard zuzugreifen.

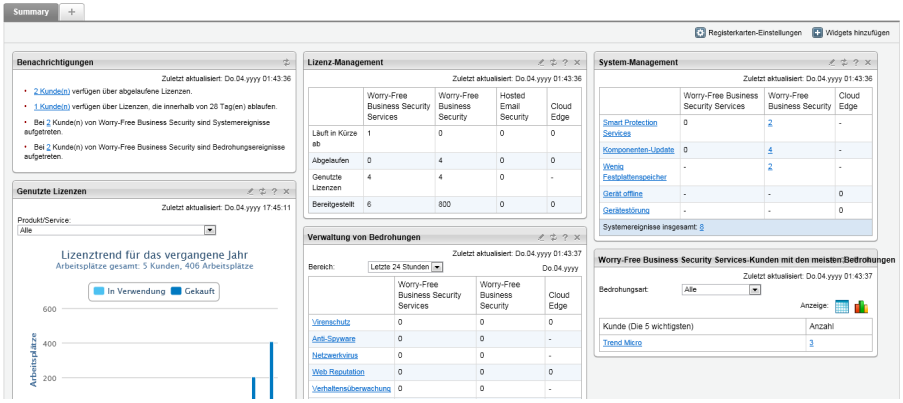


ABBILDUNG 3-1. Dashboard-Registerkarte "Bedrohungsstatus"

Die meisten Elemente im Dashboard sind verknüpft, um Sie bei der Lösung von Problemen zu unterstützen. Klicken Sie auf ein Element (Grafik, Link, Zahl), um das Problem zu beheben. Weitere Informationen zu möglichen Aktionen finden Sie unter *Produkt-/Service-Information auf Seite 3-22*.

Registerkarten und Widgets

Registerkarten stellen einen Container für Widgets bereit. Jede Registerkarte im Fenster **Zusammenfassung** kann bis zu 20 Widgets umfassen. Im Fenster **Zusammenfassung** selbst werden bis zu 30 Registerkarten unterstützt.

Widgets sind die Basiskomponenten des Dashboards. Die Widgets stellen spezifische Informationen zu verschiedenen sicherheits- oder lizenzbezogenen Ereignissen bereit. Mit einigen Widgets können spezifische Aufgaben ausgeführt werden.

Die Informationen, die von einem Widget angezeigt werden, stammen von:

- Worry-Free Business Security Server und Clients
- Worry-Free Business Security Services Server
- Hosted Email Security Services
- Cloud Edge-Servern und -Clients

Registerkartenaufgaben

In der folgenden Tabelle sind alle registerkartenbezogenen Aufgaben aufgelistet:

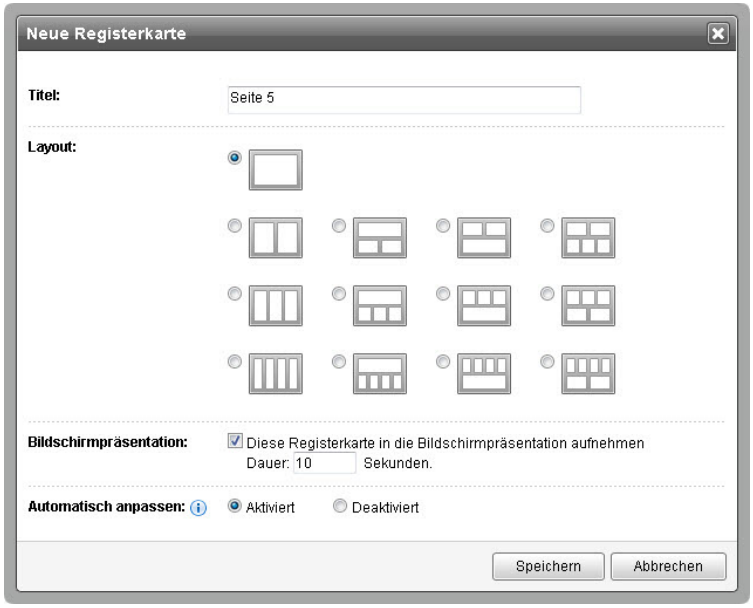
TASK	SCHRITTE
Registerkarte hinzufügen	Klicken Sie oben im Fenster **Zusammenfassung** auf das Plus-Symbol (+). Das Fenster **Neue Registerkarte** wird angezeigt.
Registerkarteneinstellungen bearbeiten	Klicken Sie auf **Registerkarteneinstellungen**. Ein Fenster, das dem Fenster **Neue Registerkarte** ähnelt, wird geöffnet, in dem Sie die Einstellungen bearbeiten können.
Bildschirmpräsentation mit Registerkarte wiedergeben	Klicken Sie auf **Bildschirmpräsentation mit Registerkarte wiedergeben**. Die Informationen in den ausgewählten Registerkarten ändern sich ähnlich wie bei einer Diaschau.
Registerkarte verschieben	Ändern Sie mit Drag & Drop die Position einer Registerkarte.

Task	Schritte
Registerkarte löschen	Klicken Sie auf das Symbol "Löschen" ( ) neben dem Registerkartentitel. Durch das Löschen einer Registerkarte werden auch alle Widgets auf der Registerkarte gelöscht.

Fenster „Neue Registerkarte“

Das Fenster **Neue Registerkarte** wird beim Hinzufügen einer neuen Registerkarte im Bildschirm **Zusammenfassung** angezeigt.

Dieses Fenster enthält die folgenden Optionen:



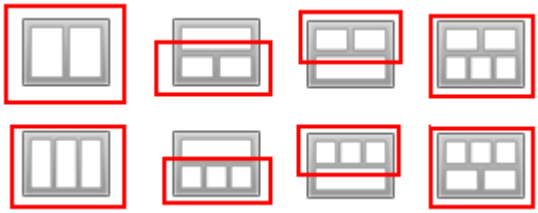
Optionen	Schritte
Titel	Geben Sie den Namen der Registerkarte ein.

Optionen	Schritte
Layout	Wählen Sie eines der verfügbaren Layouts aus.
Bildschirmpräsentation	Die Informationen in den ausgewählten Registerkarten ändern sich ähnlich wie bei einer Diaschau. Bei Aktivierung dieser Option können Sie auswählen, welche Registerkarten in der Diaschau gezeigt werden sollen und mit welcher Geschwindigkeit die Diaschau ablaufen soll.
Automatisch anpassen	Hiermit wird ein Widget an die Größe eines Felds angepasst.

Aufgaben (Widget)

In der folgenden Tabelle sind alle Widget-bezogenen Aufgaben aufgelistet:

Task	Schritte
Widget hinzufügen	Öffnen Sie eine Registerkarte und klicken Sie dann in der oberen rechten Ecke der Registerkarte auf **Widgets hinzufügen**. Das Fenster **Widgets hinzufügen** wird angezeigt.
Widgetdaten aktualisieren	Klicken Sie auf das Symbol "Aktualisieren" ( ).
Hilfe anzeigen	Klicken Sie auf **Hilfe** ( ).
Widget löschen	Klicken Sie auf das Symbol **Widget schließen** ( ). Mit dieser Aktion wird das Widget aus der Registerkarte, in der es enthalten war, gelöscht. Es wird jedoch nicht von den anderen Registerkarten gelöscht, in denen das Widget enthalten ist, und auch nicht aus der Widgetliste im Fenster **Widgets hinzufügen**.
Widget verschieben	Mit Hilfe von Drag & Drop können Sie ein Widget an eine andere Position auf der Registerkarte verschieben.

Task	Schritte
Größe eines Widgets anpassen	Sie können die Größe eines Widgets anpassen, indem Sie mit dem Cursor auf die rechte Ecke des Widgets zeigen. Wenn eine dicke senkrechte Linie und ein Pfeil angezeigt werden (siehe folgende Abbildung), halten Sie den Cursor und verschieben Sie ihn nach rechts oder links. Es können nur Widgets auf Registerkarten mit mehreren Spalten in der Größe angepasst werden. Diese Registerkarten zeichnen sich durch eines der folgenden Layouts aus. Die markierten Abschnitte enthalten Widgets, für die eine Größenanpassung möglich ist. 

Verfügbare Widgets

Das Dashboard zeigt die folgenden Widgets an.

Benachrichtigungen (Widget)

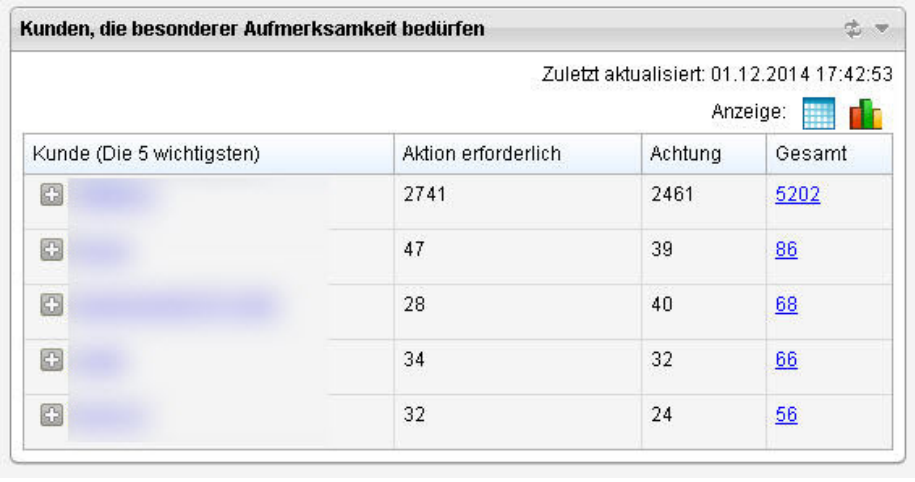
Zeigt die Ereignisse an, die eine Aktion erfordern. Dies können bedrohungsbezogene oder lizenzbezogene Ereignisse sein.

Hinweis

Dies ist ein dauerhaftes Widget, das nicht hinzugefügt oder gelöscht werden kann.

Kunden, die besonderer Aufmerksamkeit bedürfen (Widget)

Zeigt die aktuelle Anzahl der Kunden mit der höchsten Anzahl von Ereignissen an, die eine sofortige Aktivität oder Reaktion erfordern. Die Daten werden in einer Tabelle und einem Tortendiagramm angezeigt. Sie können zwischen der Tabellen- und der Tortendiagrammansicht wechseln, indem Sie auf die Anzeigesymbole ( ) klicken.

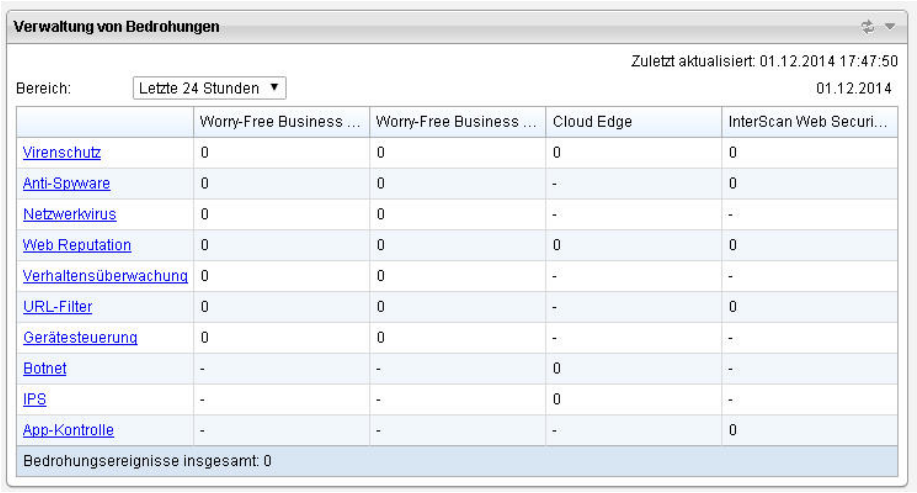


- Wenn die Anzahl der Kunden für einen spezifischen Status den Wert 1 oder höher aufweist, können Sie auf die Zahl klicken, um die Ereignisse in der Produktansicht anzuzeigen.
- Klicken Sie auf den Kundennamen, um alle Ereignisse für diesen Kunden anzuzeigen. Alternativ können Sie den Kundennamen erweitern, um Ereignisse zu bestimmten Kategorien anzuzeigen.
- Bei den Ereignissen unter **Aktion erforderlich** handelt es sich um Ereignisse, die so schnell wie möglich behandelt werden sollten.

- Bei den Ereignissen unter **Achtung** handelt es sich um Ereignisse, die nicht so dringend sind wie die Ereignisse unter "Aktion erforderlich", die jedoch so bald wie möglich behandelt werden sollten.

Verwaltung von Bedrohungen (Widget)

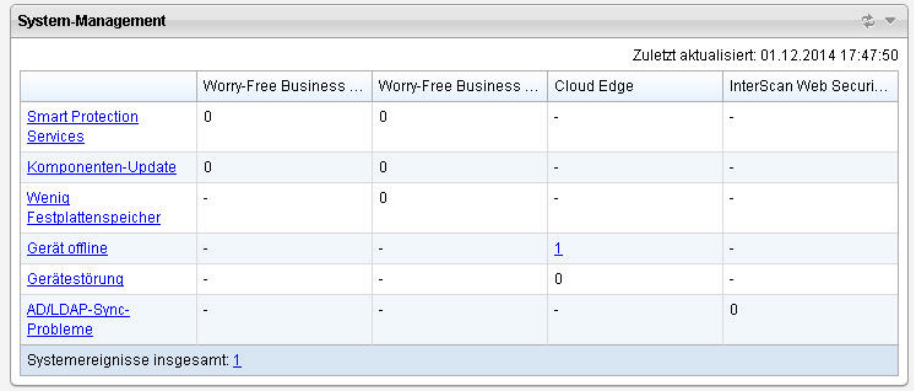
Zeigt die Anzahl der Bedrohungsereignisse für alle registrierten Produkte an.



- Sie können den Zeitraum der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:
  - Letzte 24 Stunden (Standard)
  - Letzte 7 Tage
  - Letzte 30 Tage
- Wenn die Anzahl der Ereignisse für eine spezifische Kategorie den Wert 1 oder höher aufweist, können Sie auf die Zahl klicken, um die Ereignisprotokolle anzuzeigen.

System-Management (Widget)

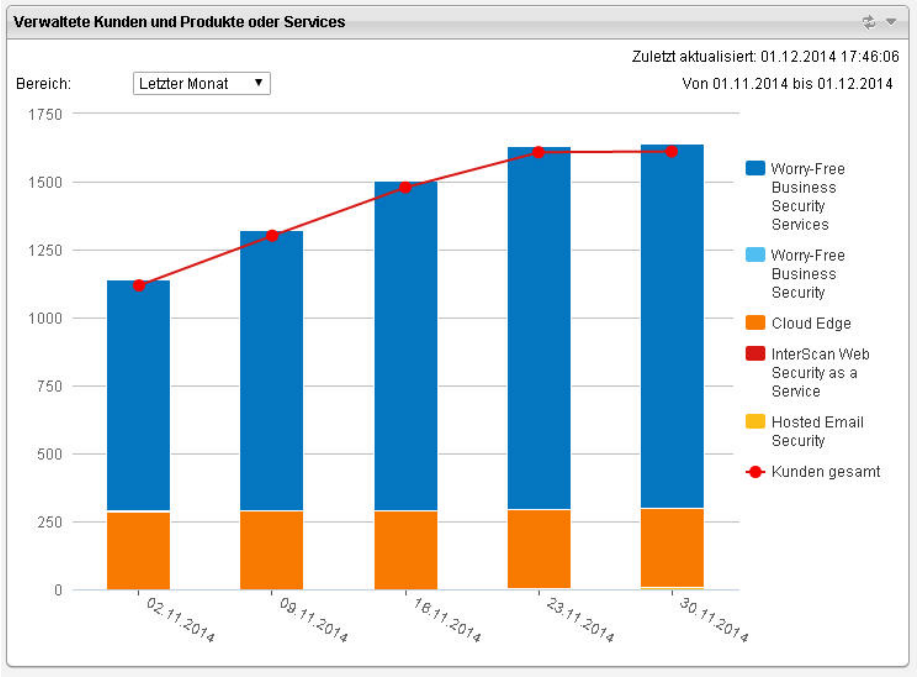
Zeigt die aktuelle Anzahl aller Systemereignisse für die registrierten Produkte an. Sie können diese Informationen nutzen, um Hardwareprobleme oder Ereignisse für den Server oder Agent zu ermitteln.



Wenn die Anzahl der Ereignisse für eine spezifische Kategorie den Wert 1 oder höher aufweist, können Sie auf die Zahl klicken, um die Ereignisprotokolle anzuzeigen.

Widget für verwaltete Kunden und Produkte oder Services

Zeigt die Anzahl der verwalteten Kunden für jedes Produkt innerhalb eines bestimmten Zeitraums an.

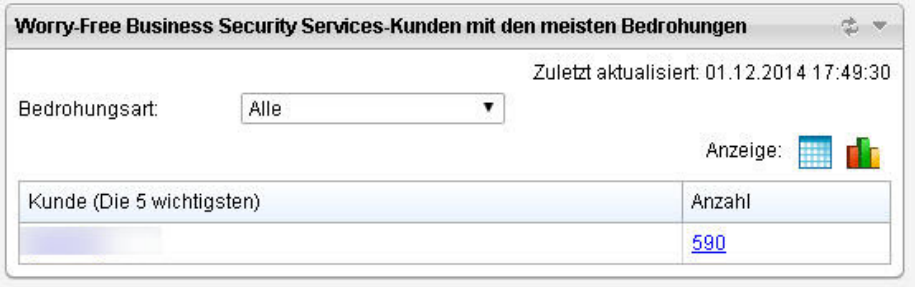


- Sie können den Zeitraum der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:
  - Letzter Monat (Standard)
  - Letzte 3 Monate
  - Letzte 6 Monate
  - Letztes Jahr

- Sie können auf die Namen der registrierten Produkte auf der rechten Seite klicken, um Daten in der Grafik hinzuzufügen oder aus der Grafik zu entfernen.
- Jedes Balkendiagramm stellt eine Woche oder einen Monat dar.
- Das Balkendiagramm zeigt die Gesamtanzahl der Produkte/Services an.

Worry-Free Business Security Services-Kunden mit den meisten Bedrohungen (Widget)

Zeigt die Worry-Free Business Security Services-Kunden mit der höchsten Anzahl von Bedrohungsereignissen an. Die Daten werden in einer Tabelle und einem Tortendiagramm angezeigt. Sie können zwischen der Tabellen- und der Tortendiagrammansicht wechseln, indem Sie auf die Anzeigesymbole ( ) klicken.



- Sie können die Bedrohungsart der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - URL-Filter
  - Verhaltensüberwachung
  - Netzwerkvirus

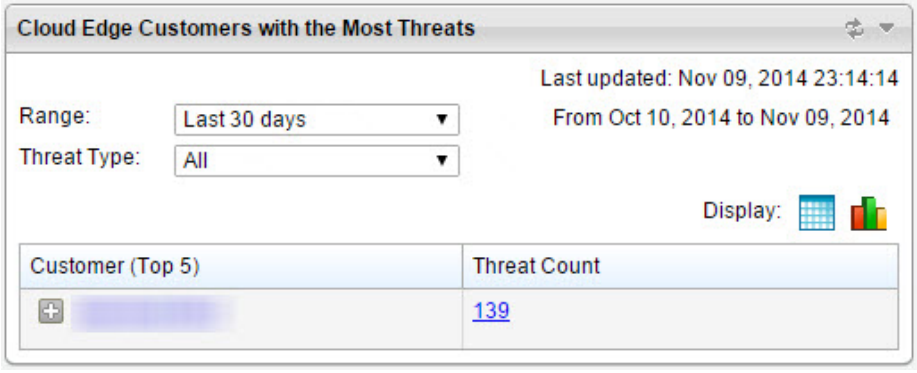
- Gerätesteuerung

- Klicken Sie auf den Namen eines Kunden, um die Kundeninformationen anzuzeigen.

- Wenn die Anzahl der Bedrohungen den Wert 1 oder höher aufweist, können Sie auf die Zahl klicken, um die Ereignisprotokolle anzuzeigen.

Cloud Edge-Kunden mit den meisten Bedrohungen (Widget)

Zeigt die Cloud Edge-Kunden mit der höchsten Anzahl von Bedrohungsereignissen an. Die Daten werden in einer Tabelle und einem Tortendiagramm angezeigt. Sie können zwischen der Tabellen- und der Tortendiagrammansicht wechseln, indem Sie auf die Anzeigesymbole ( ) klicken.



- Sie können den Zeitraum der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:

  - Letzte Stunde

  - Letzte 24 Stunden (Standard)

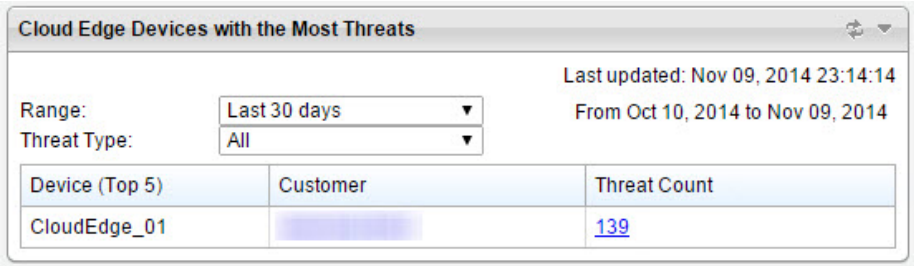
  - Letzte 7 Tage

  - Letzte 30 Tage

- Sie können die Bedrohungsart der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:
  - Alle
  - Botnet
  - Intrusion Prevention System (IPS)
  - Web Reputation
  - Virus
- Klicken Sie auf den Namen eines Kunden, um die Kundeninformationen anzuzeigen.
- Klicken Sie auf den Bedrohungszähler, um die Bedrohungsinformationen aus der Cloud Edge-Konsole anzuzeigen.

Cloud Edge-Geräte mit den meisten Bedrohungen (Widget)

Zeigt die Cloud Edge-Geräte mit der höchsten Anzahl von Bedrohungsereignissen an.

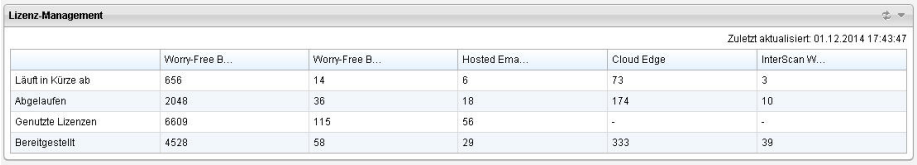


- Sie können den Zeitraum der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:
  - Letzte Stunde
  - Letzte 24 Stunden (Standard)
  - Letzte 7 Tage

  - Letzte 30 Tage
- Sie können die Bedrohungsart der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:
  - Alle
  - Botnet
  - Intrusion Prevention System (IPS)
  - Web Reputation
  - Virus
- Klicken Sie auf den Namen eines Kunden, um die Kundeninformationen anzuzeigen.
- Klicken Sie auf den Bedrohungszähler, um die Bedrohungsinformationen aus der Cloud Edge-Konsole anzuzeigen.

Lizenz-Management (Widget)

Zeigt den aktuellen Status der von den Kunden verwendeten Lizenzen an.



Es werden die folgenden lizenzbezogenen Details für Kunden und Produkte angezeigt:

- **Läuft in Kürze ab**: Dabei handelt es sich um die Lizenzen, die noch nicht abgelaufen sind, jedoch demnächst ablaufen.
- **Abgelaufen**: Dabei handelt es sich um bereits abgelaufene Lizenzen.

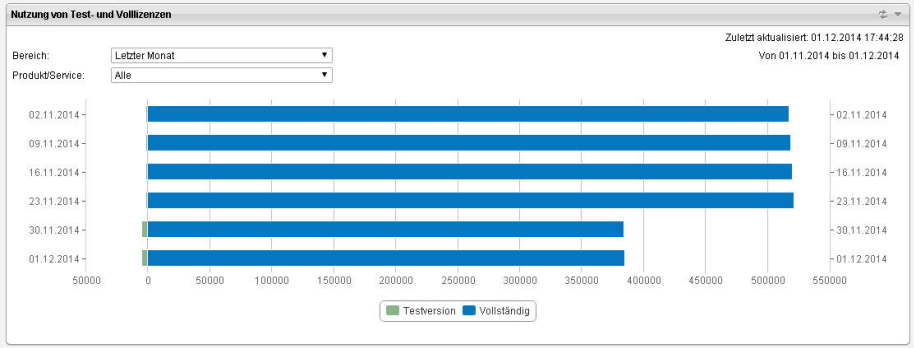
Hinweis

Trend Micro empfiehlt, diese Lizenzen schnellstmöglich zu verlängern.

- **Genutzte Lizenzen**: Dabei handelt es sich um die Arbeitsplätze, die aktuell verwendet werden.
- **Bereitgestellt**: Dabei handelt es sich um die Arbeitsplätze, die der Kunde bereitstellt.

Nutzung von Test- und Volllizenzen (Widget)

Zeigt an, wie viele Test- oder Volllizenzen für die registrierten Produkte verwendet wurden.



Sie können den Zeitraum der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:

- Letzter Monat (Standard)
- Letzte 3 Monate
- Letzte 6 Monate
- Letztes Jahr

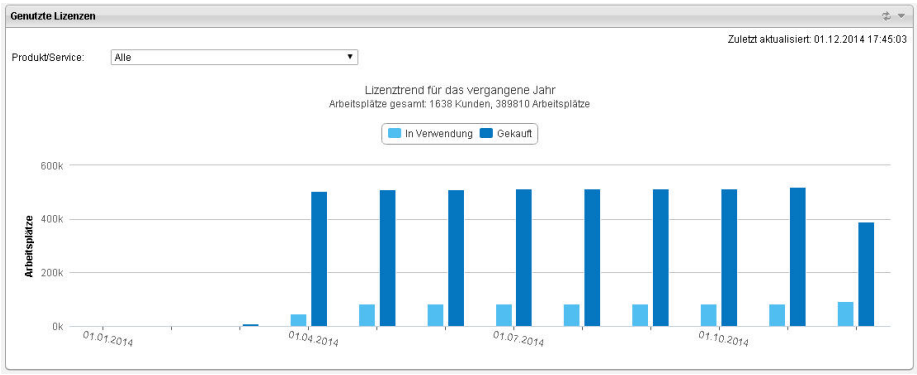
Sie können das Produkt/den Service ändern. Sie haben folgende Auswahlmöglichkeiten:

- Alle
- Hosted Email Security
- Worry-Free Business Security

- Worry-Free Business Security Services
- Cloud Edge
- InterScan Web Security as a Service

Genutzte Lizenzen (Widget)

Zeigt für das Jahr eine grafische Analyse der Arbeitsplätze an, die zugeordnet wurden, und der Arbeitsplätze, die tatsächlich gekauft wurden. Auf diese Weise können Sie besser feststellen, ob Sie die Arbeitsplatzzuordnung erhöhen oder reduzieren sollten.



Sie können das Produkt/den Service ändern. Sie haben folgende Auswahlmöglichkeiten:

- Alle
- Hosted Email Security
- Worry-Free Business Security
- Worry-Free Business Security Services
- Cloud Edge
- InterScan Web Security as a Service

InterScan Web Security as a Service-Widget

Zeigt die InterScan Web Security as a Service (IWSaaS)-Kunden mit der höchsten Anzahl von Bedrohungsereignissen an. Die Daten werden in einer Tabelle und einem Tortendiagramm angezeigt. Sie können zwischen der Tabellen- und der Tortendiagrammansicht wechseln, indem Sie auf die Anzeigesymbole ( ) klicken.

- Sie können die Bedrohungsart der angezeigten Daten ändern. Sie haben folgende Auswahlmöglichkeiten:
  - Alle
  - Antivirus
  - Anti-Spyware
  - Web Reputation
  - Anwendungskontrolle
  - URL-Filter
- Klicken Sie auf den Namen eines Kunden, um die Kundeninformationen anzuzeigen.
- Klicken Sie auf den Bedrohungszähler, um die Bedrohungsinformationen aus der IWSaaS-Konsole anzuzeigen.

Produkt-/Service-Information

Im Dashboard werden nur Kunden aufgeführt, die Aufmerksamkeit erfordern. Wenn Sie Einzelheiten zu einem beliebigen Produkt anzeigen wollen (einschließlich solcher, die im Dashboard nicht gezeigt werden), wechseln Sie zur Registerkarte **Kunden**, und rufen Sie das Produkt über die Kundenstruktur auf.

Um weitere Informationen anzuzeigen, klicken Sie auf **Kunden** > **{Kunde}** > **{Produkt}**, um weitere Informationen anzuzeigen.

Hinweis

Die angezeigten Optionen weichen für jedes Produkt/jeden Service ab.

- Worry-Free Business Security Services
  - **Gruppen**: Enthält eine Liste der konfigurierten Gruppen und der Typen.
  - **Lizenzinfo**: Zeigt alle Details der Lizenz an.
  - **Endpunkte**: Listet den Namen, die IP-Adresse, den Online/Offline-Status und die Details der Scan Engine, Pattern-Datei und der Plattform auf.
  - **Sicherheitseinstellungen**: Sicherheitseinstellungen von Worry-Free Business Security Services konfigurieren. Detaillierte Informationen finden Sie in der Dokumentation zu *Trend Micro Worry-Free Business Security Services*.

    Hinweis

    Um detailliertere Änderungen vorzunehmen, greifen Sie auf die Worry-Free Business Security Services Konsole zu.

- Worry-Free Business Security
  - **Gruppen**: Enthält eine Liste der verschiedenen auf dem Server konfigurierten Gruppen. Sie können von hier aus anfordern, eine Suche zu starten oder zu stoppen.
  - **Endpunkte**: Listet den Namen, die IP-Adresse, den Online/Offline-Status und die Details der Scan Engine, Pattern-Datei und der Plattform auf.
  - **Lizenzinfo**: Zeigt alle Details der Lizenz an.
  - **Domäneneinstellungen**: Einstellungen für die gesamte Domäne konfigurieren. Detaillierte Informationen finden Sie in der Dokumentation zu *Trend Micro Worry-Free Business Security*.

    Hinweis

    Sicherheitseinstellungen für einzelne Gruppen können hier nicht konfiguriert werden. Um diese Änderungen vorzunehmen, müssen Sie auf die Worry-Free Business Security Konsole zugreifen.

- **Verwalteter Server**: Zeigt alle Details des Servers an. Sie können von hier aus anfordern, den Server und Agents zu aktualisieren.
- **TMRM-Agent**: Enthält allgemeine Informationen zum Trend Micro Remote Manager Agent, einschließlich der Verfügbarkeit, der GUID oder des Autorisierungsschlüssels und der IP-Adresse.
- **Sicherheitseinstellungen**: Sicherheitseinstellungen einer bestimmten Gruppe konfigurieren (gilt nur für Worry-Free Business Security 6.0 und höher). Detaillierte Informationen finden Sie in der Dokumentation zu *Trend Micro Worry-Free Business Security*.

- Hosted Email Security
  - **Live-Status**: Zeigt die neuesten Informationen über Hosted Email Security an.
  - **Richtlinieneinstellungen**: Listet alle verfügbaren Richtlinien auf.
  - **Zulässige Absender**: Listet alle zugelassenen Absender auf.
  - **Lizenzinfo**: Zeigt alle Details der Lizenz an.

  Hinweis

  Um detailliertere Änderungen vorzunehmen, greifen Sie auf die Hosted Email Security Konsole zu.

- Cloud Edge

  Zeigt die neuesten Informationen über Cloud Edge an.

  Hinweis

  Um detailliertere Änderungen vorzunehmen, rufen Sie die Cloud Edge-Konsole auf.

- InterScan Web Security as a Service

  Zeigt die neuesten Informationen über InterScan Web Security as a Service an.

Hinweis

Um detailliertere Änderungen vorzunehmen, rufen Sie die InterScan Web Security as a Service-Konsole auf.

Verwaltete Produkte anzeigen

Um verwaltete Produkte anzuzeigen, klicken Sie auf **Kunden** > **{Kundenname}** > **Produkte (Registerkarte)**. Auf der Registerkarte werden in einer Strukturansicht die verwalteten Produkte der Kunden im linken Fensterbereich und ausführliche Informationen, Einstellungen und Steuerungsmöglichkeiten im rechten Fensterbereich angezeigt.

Weitere Informationen über Hosted Email Security, Worry-Free Business Security (alle), Cloud Edge und InterScan Web Security as a Service finden Sie in der jeweiligen Dokumentation unter: http://docs.trendmicro.com/de-de/home.aspx.

Kunden

Auf der Seite **Kunden** werden die Kunden und deren Produkte, die von Ihnen verwaltet werden, angezeigt. Standardmäßig werden alle Kunden in einer Tabellenansicht angezeigt. Klicken Sie auf den Firmennamen, um deren Produkte in einer Strukturansicht im linken Fensterbereich und ausführliche Informationen, Einstellungen und Steuerungsmöglichkeiten im rechten Fensterbereich anzuzeigen.

Hinweis

Weitere Informationen über Hosted Email Security, Worry-Free Business Security (alle), Cloud Edge und InterScan Web Security as a Service finden Sie in der jeweiligen Dokumentation unter: http://docs.trendmicro.com/de-de/home.aspx.

Um ein Produkt in der Kundenliste anzuzeigen, klicken Sie auf **Kunden** > **{Kundenname}** > **{Produkt}**. Sie können Folgendes konfigurieren:

- Geben Sie den Namen eines Kunden oder ein Konto ein.
- Filtern Sie die angezeigte Liste nach Kunde, Produkten, Bedrohungen, Systemen oder Lizenzereignisse.

Hinweis

Beim Filtern der Ereignisse können Sie ein, zwei oder alle Ereignisse oder Produkte auf einmal auswählen.

- Navigieren Sie mit den Navigationspfeilen durch alle Kunden.

Einige andere Aufgaben, die ausgeführt werden können:

- *Neue Kunden hinzufügen auf Seite 5-2*
- *Lizenzen für Kunden mit in Kürze ablaufenden Lizenzen oder bereits abgelaufenen Lizenzen verlängern auf Seite 7-3*
- *Berichte für bestimmte Kunden exportieren auf Seite 10-7*

Hier können Sie auch neue Kunden hinzufügen und mit der rechten Maustaste auf die meisten Knoten der Struktur klicken, um bestimmte Befehle auszuführen.

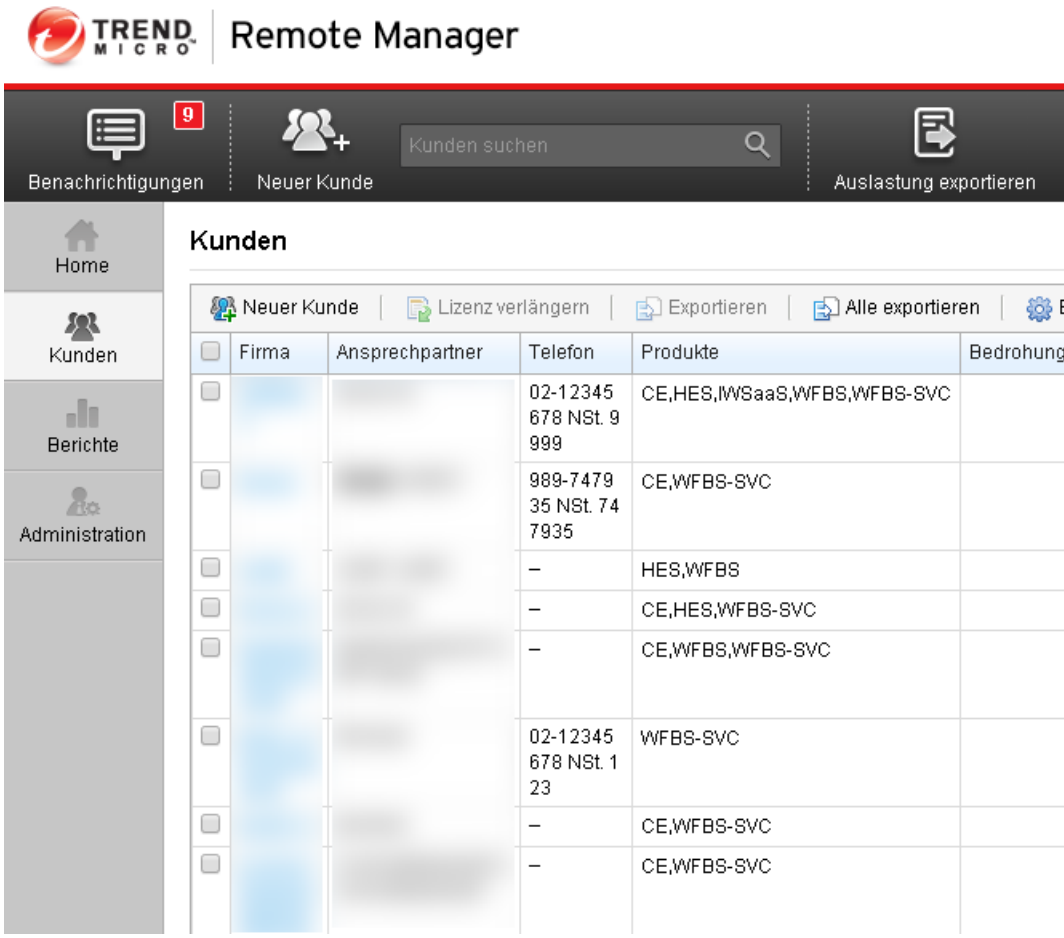


ABBILDUNG 3-2. Liste der Kunden

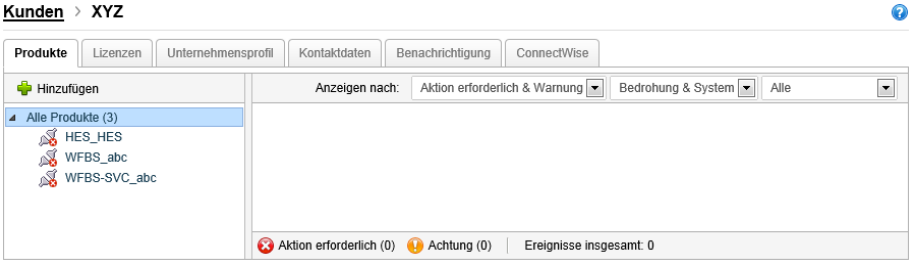


ABBILDUNG 3-3. Ansicht "Kunde"

Netzwerkstruktur

Im linken Bereich der Registerkarte **Kunden** werden die Netzwerke Ihrer Kunden in einer Baumstruktur angezeigt. Sie können nach einem Kunden suchen, alle Produkte gemeinsam oder nur Worry-Free Business Security (alle), Hosted Email Security oder Cloud Edge im Listenfeld **Anzeigen nach** anzeigen sowie mit den Navigationspfeilen durch alle Kunden navigieren. Hier können Sie auch einen Kunden hinzufügen und mit der rechten Maustaste auf die meisten Knoten der Struktur klicken, um bestimmte Befehle auszuführen. Die unten stehende Tabelle beschreibt die Objekte in der Netzwerkstruktur.

TABELLE 3-1. Objekte in der Netzwerkstruktur

SYMBOL	NETZWERKOBJEKT	BESCHREIBUNG
	Produkt/Service	Dieses Produkt/dieser Service ist nicht mit Remote Manager verbunden.
	Produkt/Service	Dieses Produkt/dieser Service ist mit Remote Manager verbunden.
	Gruppe	Servergruppe. Diese Gruppe verwaltet mehrere Client Security Agents (CSAs).
	Gruppe	Desktop-Gruppe
	Server	Servercomputer. Auf diesem Computer wird der Client Security Agent (CSA) ausgeführt.

SYMBOL	NETZWERKOBJEKT	BESCHREIBUNG
	Exchange Server	Exchange Server Computer. Auf diesem Computer wird der Messaging Security Agent (MSA) ausgeführt.
	Desktop	Desktop-Computer. Auf diesem Computer wird der Client Security Agent (CSA) ausgeführt.

Rechter Fensterbereich

Im rechten Fensterbereich wird Folgendes angezeigt:

Produkte

Auf der Registerkarte Produkte im rechten Fensterbereich sind alle Produkte eines Kunden aufgelistet. Diese Produkte können Sie über diese Registerkarte löschen. Um **Produkte** anzuzeigen, klicken Sie auf **Kunden** > **{Kundenname}** > **Produkte (Registerkarte)**. Um ein Produkt zu löschen, aktivieren Sie das links vom Produkt angezeigte Symbol, und klicken Sie auf **Löschen**. Die Registerkarte **Produkte** umfasst folgende Oberflächenelemente:

- Produktname
- Produkttyp
- Kategorie
- Vorfälle
- Details
- Status

Hinweis

Die Aktualisierung der Remote Manager Web-Konsole mit neuen Hosted Email Security Daten kann bis zu drei Stunden dauern. Hosted Email Security Kundeninformationen werden einmal pro Tag aktualisiert. Siehe *Hosted Email Security Einstellungen und Daten-Updates auf Seite 3-37*.

Lizenzen

Auf der Registerkarte **Lizenzen** werden alle einem Kunden zugeordneten Lizenzen aufgelistet. Die Registerkarte **Lizenzen** umfasst folgende Oberflächenelemente:

- Produktname
- Leistungspaket/Version
- Genutzte Lizenzen
- Bereitgestellte Lizenzen
- Ablaufdatum
- Status der automatischen Verlängerung

Status der Sicherheitseinstellungen

Der Status der Echtzeit-Sicherheitseinstellungen kann durch Klicken auf **Kunden** > **{Kundenname}** > **{Produkt} in der Netzwerkansicht** > **{Gruppe}** > **Sicherheitseinstellungen (rechter Fensterbereich)** angezeigt werden.

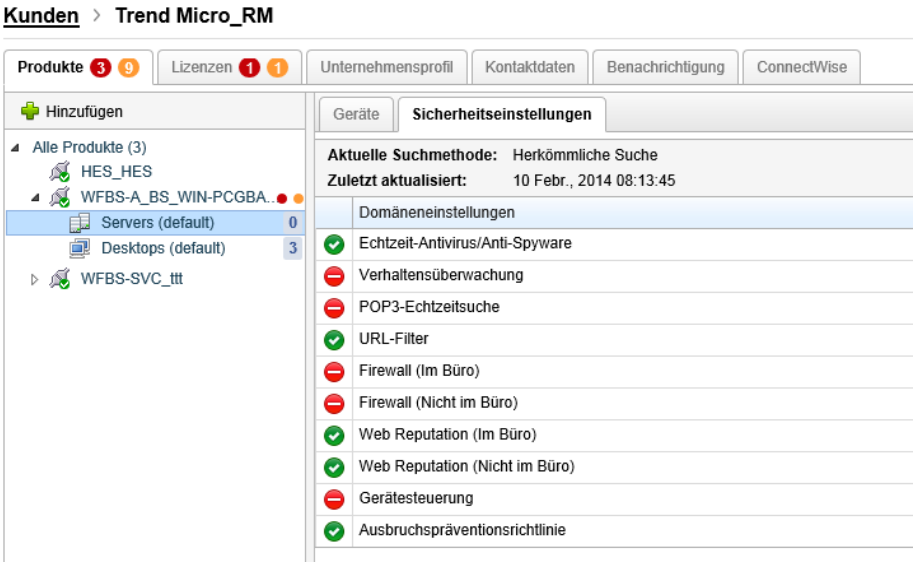


ABBILDUNG 3-4. Status der Echtzeit-Sicherheitseinstellungen

Sowohl die Einstellung "Im Büro" als auch die Einstellung "Nicht im Büro" können angezeigt werden (gilt nur für Worry-Free Business Security Standard und Worry-Free Business Security Advanced). Einstellungen werden im Listenfeld "Einstellungen" festgelegt. Einstellungen für "Nicht im Büro" sind nur relevant, wenn Location Awareness aktiviert ist.

Für weitere Informationen, siehe *Menüleiste auf Seite 3-32* und *Worry-Free Business Security Befehle auf Seite 3-34*.

Location Awareness

Mit Location Awareness (gilt nur für Worry-Free Business Security Standard und Worry-Free Business Security Advanced) können Administratoren Sicherheitseinstellungen

gemäß der Art der Verbindung des Clients mit dem Netzwerk steuern. Worry-Free Business Security Standard und Worry-Free Business Security Advanced erkennt automatisch den Standort des Clients und steuert, auf welche Websites der Benutzer zugreifen darf. Die Einschränkungen gelten je nach Standort. Worry-Free Business Security stuft Clients wie folgt ein:

- **Normale Clients**: Computer, die sich an einem festen Standort befinden und über eine ständige Netzwerkverbindung zum Security Server verfügen.
- **Roaming-Clients**: Computer, die nicht über eine ständige Netzwerkverbindung zum Security Server verfügen (z. B. Laptops). Auch die Client/Server Security Agents dieser Computer bieten Schutz vor Viren; ihr Status wird jedoch zeitverzögert an den Security Server übermittelt.

Hinweis

Location Awareness steuert die Verbindungseinstellungen für Im Büro und Nicht im Büro.

Menüleiste

Die Menü-Leiste im rechten Fensterbereich wird nur angezeigt, wenn Worry-Free oder Hosted Email Security in der Netzwerkstruktur ausgewählt wurde. Mit diesen Befehlen können Sie wichtige Aspekte der Netzwerksicherheit verwalten, wie z. B. die Einstellungen für die Echtzeitsuche und die Verteilung von Komponenten-Updates. Eine Liste der Netzwerkbefehle in der Menüleiste und Hinweise zur Verwendung dieser Befehle finden Sie unter *Worry-Free Business Security Befehle auf Seite 3-34*.

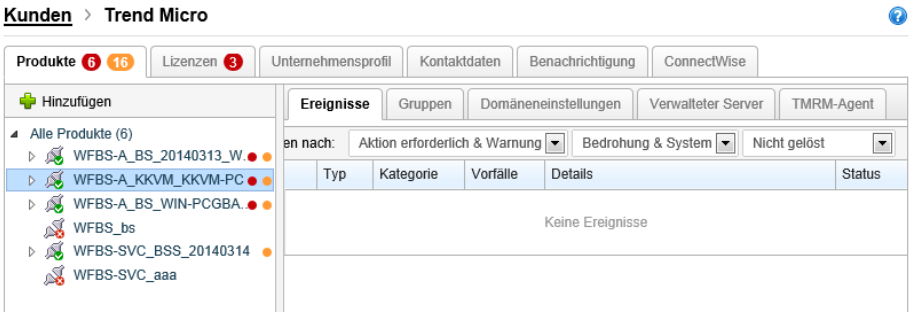


ABBILDUNG 3-5. Menüleiste

Hinweis

Wenn das gewählte Netzwerkobjekt keine Befehle empfangen kann, sind Elemente in der Menüleiste deaktiviert und reagieren nicht auf Mausklicks.

Endpunkte

Wenn Sie einen Server- oder Desktopcomputer in der Netzwerkansicht auswählen, zeigt Trend Micro Remote Manager Informationen über den Endpunkt an. Die angezeigten Informationen unterscheiden sich je nachdem, ob es sich bei diesem Endpunkt um einen Server/Desktop oder einen Exchange Server handelt. Um diese Informationen anzuzeigen, wechseln Sie zu **Kunden** > **{Kundenname}** > **{Produkt}** > **{Gruppe}** > **Geräte (rechter Fensterbereich)**. In Remote Manager™ werden die folgenden Informationen angezeigt:

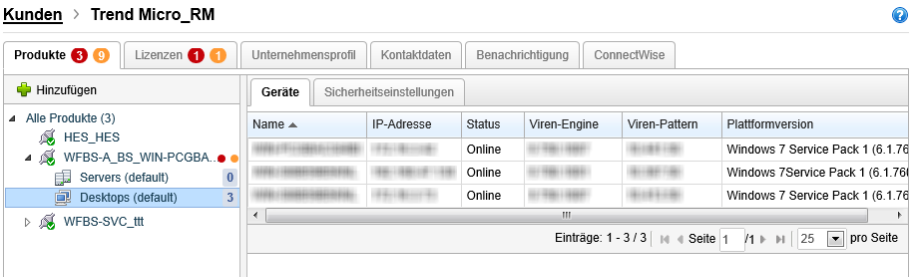


ABBILDUNG 3-6. Endpunkt-Status

- Name
- IP-Adresse
- Status
- Viren-Engine
- Viren-Pattern
- Plattformversion

Worry-Free Business Security Befehle

Mit Worry-Free Business Security (Standard und Advanced) Befehlen können Sie wichtige Sicherheitsaspekte verwalten. Hierzu zählen z. B. das Verteilen von Sicherheitskomponenten, das Durchsuchen von Computern nach Viren und bekannten Schwachstellen und Upgrades verwalteter Server.

Hinweis

Die Befehle in diesem Abschnitt stehen nur für Worry-Free Business Security (Standard und Advanced) zur Verfügung. Bei Worry-Free Business Security Services und Hosted Email Security müssen Sie sich bei der Web-Konsole dieser Produkte anmelden.

Die unten stehenden Tabellen enthalten die Worry-Free Business Security (Standard und Advanced) Befehle und deren Auswirkungen.

TABELLE 3-2. Befehle im Menü Einstellungen

BEFEHL	AKTION	AUSWIRKUNGEN
Manuelle Suche	Suche für gesamte Domäne oder Gruppe starten oder beenden.	Ermöglicht eine manuelle Suche auf Anforderung.
Jetzt aktualisieren	Verteilt die neuesten Sicherheitskomponenten, einschließlich Scan Engine und Pattern-Dateien.	Ermöglicht Komponenten-Updates nach Bedarf.
Echtzeit-Virenschutz/Anti-Spyware	Echtzeitsuche nach Viren und Spyware auf allen Computern in der Domäne aktivieren/deaktivieren.	Mit der Echtzeitsuche werden Dateien beim Zugriff automatisch durchsucht. Durch die Deaktivierung der Echtzeitsuche ist die Domäne gefährdet.
POP3-Echtzeitsuche	POP3-Echtzeitsuche für die gesamte Domäne aktivieren/deaktivieren.	POP3 Mail Scan (verfügbar im Trend Micro Anti-Spam Symbolleisten-Plug-in) schützt Computer in Echtzeit vor Sicherheitsrisiken und Spam in POP3-E-Mails.

BEFEHL	AKTION	AUSWIRKUNGEN
Verhaltensüberwachung aktivieren	Verhaltensüberwachung für die gesamte Domäne aktivieren/deaktivieren.	Die Verhaltensüberwachung schützt Computer vor unbefugten Änderungen am Betriebssystem, in Registrierungseinträgen, anderer Software oder Dateien und Ordnern.
Location Awareness	Location Awareness für die gesamte Domäne aktivieren/deaktivieren.	Mit Location Awareness können Administratoren Sicherheitseinstellungen gemäß der Art der Verbindung des Clients mit dem Netzwerk steuern. Dies betrifft Einstellungen "Im Büro/ Nicht im Büro" der Firewall, Web Reputation und TrendSecure Symbolleisten: Anti-Keylogger, Verschlüsselung von Tastatureingaben, Bewertung von Webseiten. Einstellungen für "Im Büro" sind die Standardeinstellungen, wenn Location Awareness deaktiviert ist. Einstellungen für Nicht im Büro sind nur verfügbar, wenn Location Awareness aktiviert ist.
Firewall	Personal Firewall für die gesamte Domain aktivieren/deaktivieren.	Je nach bestehenden Firewall-Regeln kann die Aktivierung einer Firewall die Kommunikation von Computern mit dem Netzwerk beeinträchtigen. Die Deaktivierung kann den Computer unerwünschtem Netzwerkverkehr aussetzen.
Web Reputation	Web Reputation für die gesamte Domäne konfigurieren.	Durch den Abgleich aller angeforderten Links mit der Trend Micro Web Security Datenbank kann Web Reputation den Zugriff auf Links, die potenzielle Sicherheitsrisiken darstellen, verhindern.

BEFEHL	AKTION	AUSWIRKUNGEN
URL-Filter	URL-Filter für die gesamte Domäne aktivieren/deaktivieren.	Bei aktiviertem URL-Filter werden die Versuche, auf nicht autorisierte Webseiten zuzugreifen, überwacht. Dies ist nur für Worry-Free Business Security Services und Worry-Free Business Security Advanced 6.0 und höher verfügbar.
Gerätesteuerung	Gerätesteuerung für die gesamte Domäne aktivieren/deaktivieren.	Bei aktivierter Gerätesteuerung werden die Versuche, ohne Autorisierung auf Geräte zuzugreifen, überwacht. Dies ist nur für Worry-Free Business Security Advanced 7.x und 8.0 verfügbar.
Schwachstellenbewertung starten	Schwachstellenbewertung starten, um Computer in der Domäne nach bekannten Sicherheitslücken zu durchsuchen.	Verbraucht einige Ressourcen auf Computern und führt zu einem leichten Anstieg des Datenverkehrs zwischen dem verwalteten Server und den Computern.
Damage Cleanup Service starten	Verteilt die Damage Cleanup Services (DCS), um infizierte Computer zu säubern.	Verbraucht einige Ressourcen auf Computern und kann zu einem leichten Anstieg des Datenverkehrs zwischen dem verwalteten Server und den Computern führen.
Verwalteten Server aktualisieren	Verteilt die aktuellen Sicherheitskomponenten einschließlich Scan Engine und Pattern-Dateien ausschließlich auf dem verwalteten Server.	Stellt sicher, dass auf den Computern die aktuellen Sicherheitskomponenten ausgeführt werden. Die Verteilung kann den Datenverkehr zwischen Computern und dem verwalteten Server erhöhen.

BEFEHL	AKTION	AUSWIRKUNGEN
Client Server Security Agent aktualisieren	Die aktuellen Sicherheitskomponenten einschließlich Scan Engine und Pattern-Dateien auf alle Client Server Security Agents (CSA) in der Domäne verteilen.	Stellt sicher, dass auf den Computern die aktuellen Sicherheitskomponenten ausgeführt werden. Die Verteilung kann den Datenverkehr zwischen Computern und dem verwalteten Server erhöhen.

Hosted Email Security Einstellungen und Daten-Updates

Um Hosted Email Security Einstellungen und Informationen einschließlich Live-Status, Allgemeine Einstellungen und Info über anzuzeigen, klicken Sie auf **Kunden (Registerkarte)** > **{Kunde}** > **Hosted Email Security**.

Die folgenden Details werden für alle Domänen aufgelistet und einmal täglich aktualisiert:

- Alle Informationen unter der Registerkarte **Live-Status**.
- **Richtlinieneinstellungen**
- **Zulässige Absender**
- Alle Informationen unter der Registerkarte **Lizenzinfo**.

Hinweis

Die Aktualisierung der Remote Manager Web-Konsole mit neuen Hosted Email Security Daten kann bis zu drei Stunden dauern.

Benachrichtigungen

Kundenbenachrichtigungen können per E-Mail gesendet werden oder über das Widget **Benachrichtigungen** oder die Software eines Drittanbieters angezeigt werden.

Das Fenster **Benachrichtigungen konfigurieren** wird angezeigt. In diesem Fenster können Sie Folgendes festlegen:

- Ereignisse, die Benachrichtigungen auslösen:
  - Lizenzbezogene Ereignisse:
    - **Läuft in Kürze ab**: Bei in Kürze ablaufenden Lizenzen eine Benachrichtigung senden. Sie können auch festlegen, wie oft das System eine Benachrichtigung versenden soll.
      - **Monatlich**: Vom System wird alle 30 Tage eine E-Mail-Benachrichtigung gesendet, beginnend ab 60 Tage vor Ablauf der Lizenz.
      - **Vierzehntäglich**: Vom System wird alle 14 Tage eine E-Mail-Benachrichtigung gesendet, beginnend ab 28 Tage vor Ablauf der Lizenz.
      - **Wöchentlich**: Vom System wird alle 7 Tage eine E-Mail-Benachrichtigung gesendet, beginnend ab 14 Tage vor Ablauf der Lizenz.

Hinweis

Obwohl Sie festgelegt haben, dass die Benachrichtigung per E-Mail wöchentlich, vierzehntäglich oder monatlich gesendet wird, erhalten Sie möglicherweise täglich eine E-Mail-Benachrichtigung, da diese vom Ablaufdatum der Lizenzen eines Unternehmens abhängig ist. Wenn Sie jedoch sicherstellen möchten, dass Sie nicht mehrere E-Mail-Benachrichtigungen am selben Tag erhalten, fügt Trend Micro auch die Firmennamen und Daten anderer Produkte, die in Kürze ablaufen werden, in dieselbe E-Mail ein.

    - **Abgelaufen**: Bei bereits abgelaufenen Lizenzen eine Benachrichtigung senden.
    - **Überschrittene Zuordnung**: Benachrichtigung senden, wenn der Prozentsatz der genutzten Lizenzen die Anzahl der bereitgestellten Arbeitsplatzlizenzen überschreitet. Sie können den Prozentsatz der genutzten Arbeitsplatzlizenzen festlegen, die die vom Kunden bereitgestellten Arbeitsplätze überschritten haben. Das kann ein beliebiger Wert zwischen 100 und 120 sein.
  - Produktbezogene Ereignisse:

- Worry-Free Business Security- und Worry-Free Business Security Services-Ereignisse:
  - **Bedrohungen**: Benachrichtigung senden, wenn die Anzahl der Bedrohungsereignisse den festgelegten Schwellenwert überschritten hat.
  - **System**: Benachrichtigung senden, wenn die Anzahl der System- oder Geräteereignisse den festgelegten Schwellenwert überschritten hat.
- Cloud Edge-Ereignisse:
  - **Überschrittene Internet-Bedrohungen entdeckt**: Benachrichtigung senden, wenn die Anzahl der Internet-Bedrohungen den festgelegten Schwellenwert überschritten hat.

- Empfänger der Benachrichtigung:
  - **Kaseya** (Nur Worry-Free Business Security- und Worry-Free Business Security Services-Ereignisse)
  - **Autotask** (Nur Worry-Free Business Security- und Worry-Free Business Security Services-Ereignisse)
  - **ConnectWise**
  - **Ich**: An diese E-Mail-Adresse wird die E-Mail-Benachrichtigung gesendet.

Hinweis

Wenn die E-Mail-Adresse ungültig ist, klicken Sie auf den Link **Licensing Management Platform** oder auf die Schaltfläche **Mein Konto**, um zur Seite mit den Profileinstellungen zu wechseln und die Einstellungen für das Profil zu ändern.

  - **Zusätzliche Empfänger**: Sie können zusätzliche E-Mail-Empfänger für kundenspezifische Ereignisse festlegen.

Weitere Informationen zum Konfigurieren von Benachrichtigungen finden Sie unter *Benachrichtigungen konfigurieren auf Seite 8-2*.

Worry-Free Business Security Services Status und Daten-Updates

Um Worry-Free Business Security Services-Einstellungen und -Daten sowie den Status anzuzeigen, klicken Sie auf **Kunden** > **{Kundenname}** > **{Produkt}** > **WFBS-SVC**.

Die Worry-Free Business Security Services-Informationen werden einmal pro Tag aktualisiert. Dazu zählen:

- Alle Informationen unter **Sicherheitseinstellungen**.
- Das **Ablaufdatum**auf der Registerkarte **Lizenzinfo** (dies ist das Ablaufdatum für den Worry-Free Business Security Services-Aktivierungscode).

Hinweis

Die Aktualisierung der Remote Manager Web-Konsole mit neuen Worry-Free Business Security Services-Daten kann bis zu drei Stunden dauern.

Je nach Ihrem Lizenzmechanismus können andere Optionen angezeigt werden.

Kapitel 4

Infrastruktur einrichten

Dieser Abschnitt enthält die folgenden Themen:

- *Überblick über die Installation der Infrastruktur auf Seite 4-2*
- *Produkte hinzufügen auf Seite 4-4*

Überblick über die Installation der Infrastruktur

Im Allgemeinen beinhaltet die Vorbereitung der Service-Infrastruktur die folgenden Schritte für jeden Produkt-/Servicetyp.

Worry-Free Business Security Standard und Worry-Free Business Security Advanced

1. Einen neuen Kunden zur Remote Manager Web-Konsole hinzufügen.
2. Den Hauptkundenkontakt hinzufügen.
3. Fügen Sie mindestens ein Produkt zu diesem Kundenkonto hinzu.
4. Den Agent auf dem Server des Kunden installieren.
5. Geben Sie die GUID oder den Autorisierungsschlüssel im Agent ein.

Hosted Email Security und Worry-Free Business Security Services

1. Einen neuen Kunden zur Remote Manager Web-Konsole hinzufügen.
2. Den Hauptkundenkontakt hinzufügen.
3. Fügen Sie mindestens einen Dienst zu diesem Kundenkonto hinzu.
4. Den Autorisierungsschlüssel auf der Service-Konsole des Kunden eingeben.

InterScan Web Security as a Service (IWSaaS)

1. Einen neuen Kunden zur Remote Manager Web-Konsole hinzufügen.
2. Den IWSaaS-Dienst zu diesem Kundenkonto hinzufügen.

Hinweis

Da Ihr IWSaaS-Konto bereits mit der Licensing Management Platform verknüpft ist, müssen Sie zur Anmeldung bei IWSaaS keine Anmeldedaten eingeben.

ConnectWise

1. Verküpfen Sie ConnectWise und fügen Sie die ConnectWise Anmeldedaten in der Remote Manager Web-Konsole unter **Administration** > **Integration anderer Anbieter konfigurieren (Bildschirm)** hinzu.
2. Geben Sie die allgemeinen ConnectWise-Benachrichtigungseinstellungen an.
3. Fügen Sie den Empfänger der Benachrichtigung zur Empfängerliste unter **Kunden** > **{Kunde}** > **Benachrichtigung (Registerkarte)** in der Remote Manager Web-Konsole hinzu.
4. Fügen Sie die erforderlichen Felder zur ConnectWise-Konsole hinzu.
5. (Optional) Konfigurieren Sie die ConnectWise-Einstellungen und -Benachrichtigungen für jeden Kunden.

Kaseya

1. Verknüpfen Sie Kaseya und fügen Sie die Kaseya E-Mail-Adresse des Benutzers in der Remote Manager Web-Konsole unter **Administration** > **Integration anderer Anbieter konfigurieren (Bildschirm)** hinzu.
2. Fügen Sie den Empfänger der Benachrichtigung zur Empfängerliste unter **Kunden** > **{Kunde}** > **Benachrichtigung (Registerkarte)** in der Remote Manager Web-Konsole hinzu.
3. Die erforderlichen Felder zur Kaseya Konsole hinzufügen.

Autotask

1. Verküpfen Sie Autotask und fügen Sie die Autotask Anmeldedaten in der Remote Manager Web-Konsole unter **Administration** > **Integration anderer Anbieter konfigurieren (Bildschirm)** hinzu.

2. Fügen Sie den Empfänger der Benachrichtigung zur Empfängerliste unter **Kunden** > **{Kunde}** > **Benachrichtigung (Registerkarte)** in der Remote Manager Web-Konsole hinzu.

3. Die erforderlichen Felder zur Autotask Konsole hinzufügen.

Produkte hinzufügen

Fügen Sie den Kunden hinzu, bevor Sie zu diesem Kundenkonto Produkte hinzufügen.

Kunden hinzufügen

Vor der Erstellung des Kundenkontos sollten Sie grundsätzliche Kundendaten erfassen. Dazu zählen **Vor- und Nachname** (wie er auf Berichten und Benachrichtigungen erscheint), **Zeitzone** (des Kunden) und **Sprache** (in der der Kunde Berichte und Benachrichtigungen erhält). Vergewissern Sie sich vor dem Hinzufügen eines Kunden und Installieren des Agents auf dem verwalteten Server, dass Sie die schriftliche Zustimmung zur Durchführung von Aufgaben zum Überwachen, Verwalten und Zugriff auf die Ressourcen des Kunden haben.

Prozedur

1. Klicken Sie über das Remote Manager Web-Konsolenbanner auf **Neuer Kunde**.

Hinweis

Sie können über das Banner oder über die Registerkarte **Kunden** auf **Neuer Kunde** klicken.

2. Geben Sie die Kundeninformationen an.

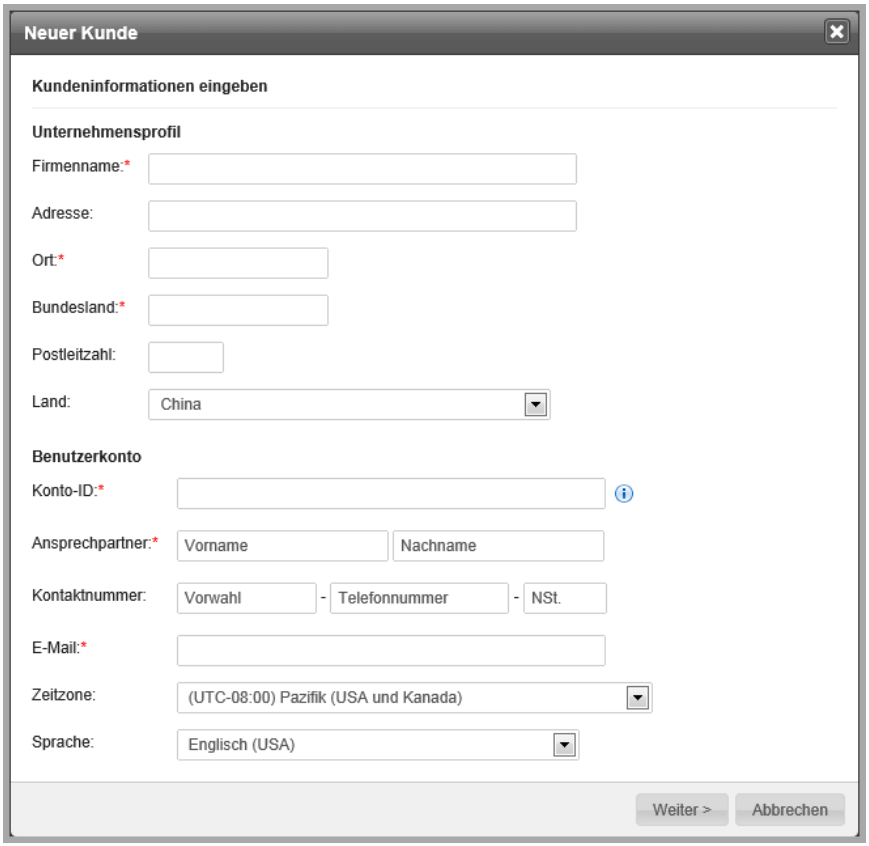
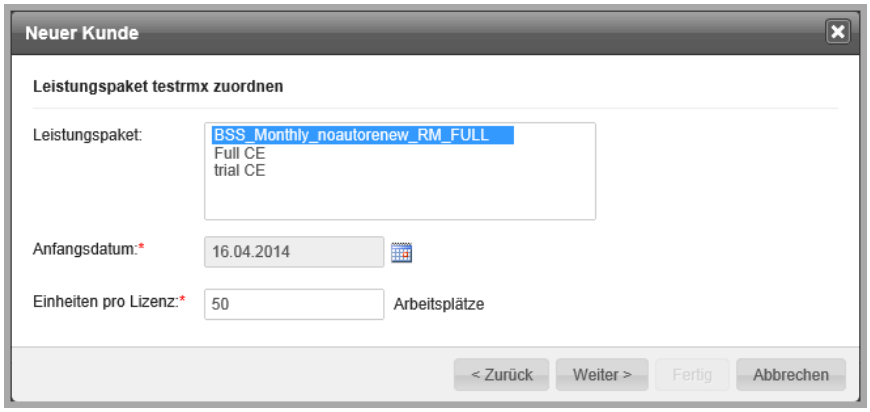


ABBILDUNG 4-1. Fenster Kunden-Info

3. Klicken Sie auf **Weiter >**.

4. Ordnen Sie ein Leistungspaket, ein Anfangsdatum der Lizenz und die Anzahl der Einheiten pro Lizenz zu.



5. Konfigurieren Sie die Standardeinstellungen für das Produkt für dieses Konto. Diese Einstellungen sind:

Hinweis

Diese Funktion ist nur für Worry-Free Business Security Services vorgesehen.

- **Grundlegende Produkteinstellungen**: Konfigurieren Sie nur die Einstellungen in diesem Fenster, die neue Kundenkonten verwenden.

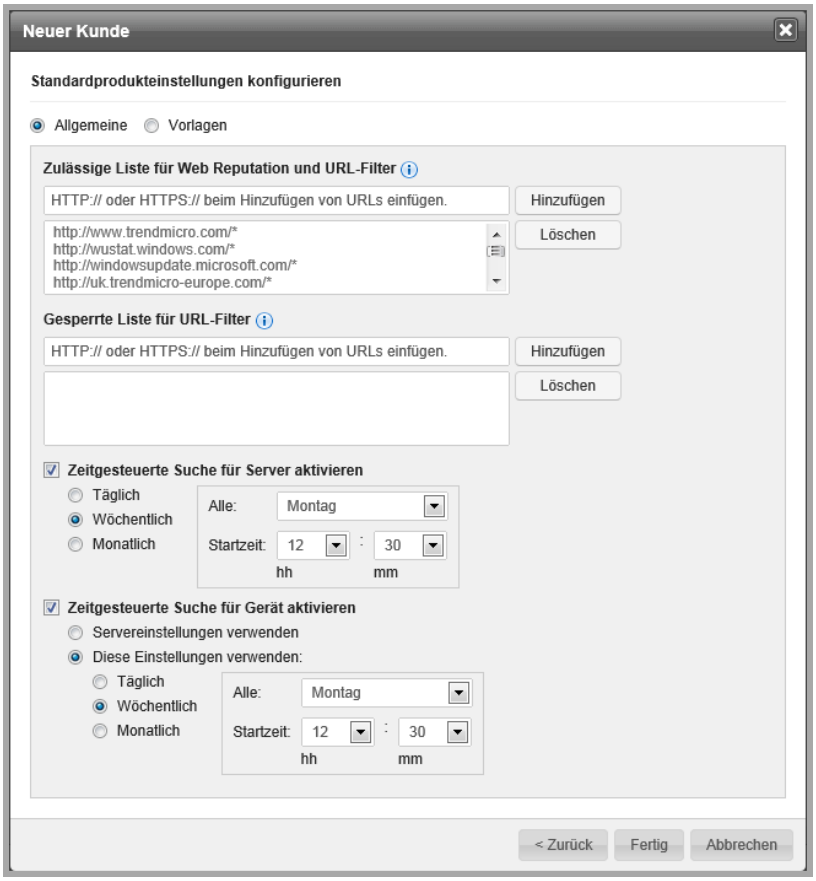


ABBILDUNG 4-2. Grundlegende Produkteinstellungen

- **Vorlagen**: Verwenden Sie diese Option, um eine Vorlage mit Standardeinstellungen auszuwählen. Konfigurieren Sie die Standardeinstellungen über **Admin** > **Vorlage für Standardeinstellungen konfigurieren**.

6. Überprüfen Sie die Informationen und klicken Sie dann auf **Fertig**.

Hinweis

Nachdem der Kunde hinzugefügt wurde, können Profiländerungen nur über die Trend Micro Licensing Management Platform vorgenommen werden.

Trend Micro Produkte bei Trend Micro Remote Manager registrieren

Sie können Trend Micro Produkte bei Trend Micro Remote Manager registrieren. Weitere Informationen zu Drittanbieterprodukten finden Sie unter *Produkte anderer Hersteller in Trend Micro Remote Manager integrieren auf Seite 4-16*.

Worry-Free Business Security registrieren

Dieser Abschnitt gibt Aufschluss darüber, wie Sie eine Verbindung der Worry-Free Business Security über Trend Micro Remote Manager herstellen bzw. trennen können.

Agent-GUID oder Autorisierungsschlüssel

Um zwischen Produkten und Services zu unterscheiden, weist Remote Manager jedem Produkt und jedem Service eine GUID oder einen Autorisierungsschlüssel zu. Wenn Sie der Remote Manager Web-Konsole ein Produkt oder einen Service hinzufügen, generiert Remote Manager jedes Mal eine neue GUID oder einen neuen Autorisierungsschlüssel. Während der Installation des Agents auf dem verwalteten Server oder beim Hinzufügen des Service zur Remote Manager Web-Konsole muss die GUID oder der Autorisierungsschlüssel eingegeben werden, damit das Produkt bei Remote Manager registriert werden kann.

Die GUID oder der Autorisierungsschlüssel für die Produkte/Services eines Kunden sind immer erhältlich über: **Kunden** > **Alle Kunden (in der Struktur)** > **{Kunde}** > **TMRM Agent (Registerkarte)**.

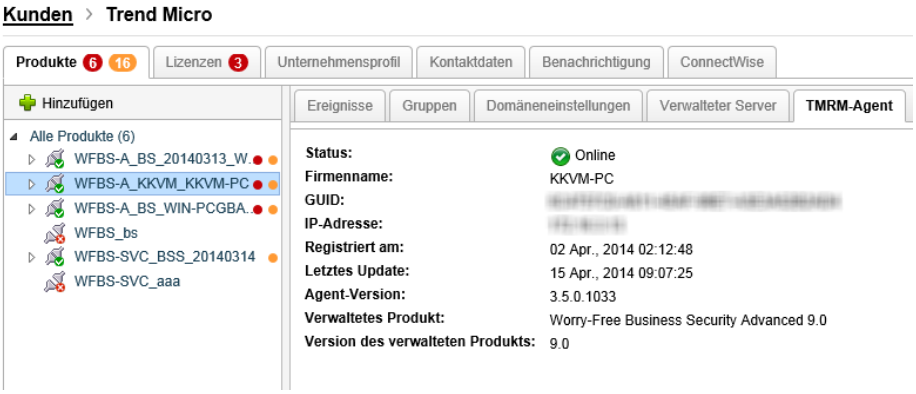


ABBILDUNG 4-3. Die Agent-GUID oder der Autorisierungsschlüssel sind immer verfügbar (Worry-Free Business Security Standard und Advanced)

Remote ManagerAgent-GUID

```
1A2B3C4567D8-E1FGHI23-J456-78K9-1L23
```

Agent-Installation für Worry-Free Business Security 6,0 und höher

Es gibt verschiedene Möglichkeiten, um den Trend Micro Remote Manager Agent auf dem Server mit Worry-Free Business Security Standard oder Advanced, Version 6.0 oder höher, zu installieren. Die Installationsvorgänge sind davon abhängig, ob der Kunde neu ist oder bereits über ein Konto in der Remote Manager Web-Konsole verfügt.

Vorbereitung zur Installation

- Remote ManagerAgent-GUID
- Agent-Installationsprogramm (`WFRMAgentforWFBS.exe`)

- Aktive Internet-Verbindung
- 50 MB verfügbarer Festplattenspeicher

Kunden ohne Remote Manager-Konten

Prozedur

- Möglichkeit 1: Über die Remote Manager Web-Konsole

  1. Fügen Sie über Remote Manager Web-Konsole Kunden hinzu und geben Sie eine optionale Beschreibung an.
  2. Fügen Sie Worry-Free Business Security Standard oder Advanced zur Remote Manager Web-Konsole hinzu, wobei eine GUID generiert wird.
  3. Installieren Sie den Remote Manager Agent mit Hilfe der in der Konsole generierten GUID auf dem Worry-Free Business Security Standard oder Advanced Server.

- Möglichkeit 2: Installieren Sie den Agent auf dem Worry-Free Business Security Server.

  Verwenden Sie das Remote Manager Agent-Installationsprogramm auf dem Worry-Free Business Security Server (ohne den Kunden vorher der Remote Manager Web-Konsole hinzuzufügen), um den Agent zu installieren.

Kunden mit Remote Manager-Konten

Prozedur

1. Fügen Sie Worry-Free Business Security Standard oder Advanced zur Remote Manager Web-Konsole hinzu, wobei eine GUID generiert wird.
2. Installieren Sie den Remote Manager Agent mit Hilfe der in der Konsole generierten GUID auf dem Worry-Free Business Security Standard oder Advanced Server.

Trend Micro Remote Manager Agent-Installation überprüfen

Überprüfen Sie, dass der Agent erfolgreich installiert wurde.

Agent-Dienst-Status überprüfen

Überprüfen Sie, ob auf dem Computer, auf dem der Remote Manager Agent installiert ist, `Trend Micro Information Center for CSM` gestartet wurde.

Prozedur

1. Klicken Sie auf **Start** > **Einstellungen** > **Systemsteuerung** > **Administrator-Tools** > **Services**.
2. Suchen Sie den **Trend Micro Remote Manager Agent**.
3. Der **Status** muss **Gestartet** sein.

Startmenü-Verknüpfungen überprüfen

Überprüfen Sie auf dem Computer, auf dem der Trend Micro Remote Manager Agent installiert ist, die Programmgruppe im Start-Menü.

Prozedur

1. Klicken Sie auf **Start** > **Programme** > **Trend Micro Remote Manager Agent**.
2. Prüfen Sie, ob die Programmgruppe die folgenden Einträge enthält:
   - Agent-Konfigurationstool
   - Readme

Symbol in der Task-Leiste überprüfen

Überprüfen Sie auf dem Computer, auf dem der Trend Micro Remote Manager Agent installiert ist, das Symbol des Trend Micro Remote Manager Agents in der Task-Leiste. Sollte das Symbol aus irgendeinem Grund nicht angezeigt werden, können Sie es durch Klicken auf **Start** > **Programme** > **Trend Micro Remote Manager Agent** > **Agent-Konfigurationstool** starten.

Durch das Beenden des Tools wird der Trend Micro Remote Manager Service nicht beendet. Es wird nur das Konfigurationstool geschlossen und das Symbol aus der Task-Leiste entfernt. Das Tool kann jederzeit erneut gestartet werden.

Halten Sie zur Anzeige von Statusinformationen die Maus über das Symbol.

TABELLE 4-1. Symbole der Task-Leiste

SYMBOL	BESCHREIBUNG
	Ein grünes Symbol zeigt an, dass der Agent mit dem Kommunikationsserver von Trend Micro Remote Manager verbunden ist. Der Agent wird ordnungsgemäß ausgeführt.
	Ein rotes Symbol zeigt an, dass der Agent nicht mit dem Kommunikationsserver von Trend Micro Remote Manager verbunden ist oder die Version des Agents nicht mit der des Servers übereinstimmt und aktualisiert werden muss.
	Ein rotes Symbol mit einem roten Pfeil zeigt an, dass der Agent von Trend Micro Remote Manager abgemeldet ist.
	Ein Symbol mit einem roten "X" bedeutet, dass der Agent deaktiviert wurde.

Verbindung zwischen Agent und Server überprüfen

Um sicherzustellen, dass der Trend Micro Remote Manager Service ordnungsgemäß ausgeführt wird, müssen die Agents auf der Remote Manager Web-Konsole "verbunden" oder "online" sein.

Navigieren Sie zu **Kunden** > **{Kunde}** > **Produkte (Registerkarte)** .

In der Struktur wird der Status jedes Agents in der Spalte **Status** angezeigt. Details über jeden Status finden Sie unter *Agent-Status auf Seite 6-2*.

Zusätzlich zum aktuellen Kapitel finden Sie unter *Fehlerbehebung und bekannte Probleme auf Seite 11-1* weitere Erläuterungen von Problemen im Zusammenhang mit der Verbindung zwischen Server und Agent.

Installationsfehler anzeigen

In den Agent-Installationsprotokollen werden Aktivitäten bei der Agent-Installation aufgezeichnet. Sollten bei der Installation Probleme auftreten, senden Sie diese

Protokolle an Ihren Support-Anbieter. Die Agent-Installationsprotokolle befinden sich an folgendem Speicherort auf dem verwalteten Server:

```
C:\WFRMAgentForCSM_Install.log
```

Worry-Free Business Security Services registrieren

In diesem Abschnitt erfahren Sie, wie Sie eine Verbindung der Worry-Free Business Security Services über Trend Micro Remote Manager herstellen bzw. trennen können.

Einen Worry-Free Business Security Services-Kunden mit der Remote Manager Web-Konsole verbinden

Um Worry-Free Business Security Services über die Trend Micro Remote Manager Web-Konsole zu verwalten, muss ein Worry-Free Business Security Services-Kundenkonto bei Remote Manager registriert sein. Führen Sie dazu die folgenden Schritte aus:

Hinweis

Wenn der Reseller das Produkt Ihrem Konto über die Licensing Management Platform hinzugefügt hat, müssen Sie die folgenden Schritte nicht ausführen.

Prozedur

1. Fügen Sie das Produkt zur Remote Manager Web-Konsole hinzu und speichern Sie die GUID oder den Autorisierungsschlüssel.

   Weitere Informationen finden Sie unter *Produkte/Services hinzufügen auf Seite 5-9*.

2. Melden Sie sich beim Worry-Free Business Security Services-Konto des Kunden an.

3. Gehen Sie zu **Administration** > **Trend Micro Remote Manager**.

4. Geben Sie den Autorisierungsschlüssel ein, und klicken Sie auf **Verbinden**.

Einen Worry-Free Business Security Services-Kunden von der Remote Manager Web-Konsole trennen

So trennen Sie Worry-Free Business Security Services von der Remote Manager Web-Konsole:

- Wenn das Konto in die Licensing Management Platform integriert wurde, kann der Reseller das Leistungspaket aus der Licensing Management Platform-Web-Konsole löschen. Sobald das Leistungspaket gelöscht wurde, wird der Kunde von der Remote Manager Web-Konsole getrennt.
- Bei anderen Konten kann der Kunde den Remote Manager Bildschirm in der Worry-Free Business Security Services-Web-Konsole öffnen und auf **Trennen** klicken.

Der Kunde wird dann in der Worry-Free Business Security Services-Konsole benachrichtigt.

Hosted Email Security registrieren

In diesem Abschnitt erfahren Sie, wie Sie eine Verbindung der Hosted Email Security über Trend Micro Remote Manager herstellen bzw. trennen können.

Einen Hosted Email Security-Kunden mit der Remote Manager Web-Konsole verbinden

Um Hosted Email Security über die Trend Micro Remote Manager Web-Konsole zu verwalten, muss ein Hosted Email Security Konto bei Remote Manager registriert sein.

Hinweis

Wenn der Reseller das Produkt Ihrem Konto über die Licensing Management Platform hinzugefügt hat, müssen Sie die folgenden Schritte nicht ausführen.

Prozedur

1. Fügen Sie das Produkt zur Remote Manager Web-Konsole hinzu und speichern Sie die GUID oder den Autorisierungsschlüssel.

2. Melden Sie sich am Hosted Email Security Konto des Kunden an.
3. Wechsel Sie zu **Administration** > **Remote Manager**.
4. Geben Sie die GUID oder den Autorisierungsschlüssel ein und klicken Sie auf **Verbinden**.

   Nach Eingabe der GUID oder des Autorisierungsschlüssels und Klicken auf **Verbinden** kann es bis zu zehn Minuten dauern, bis die Verbindung von Hosted Email Security mit der Remote Manager Web-Konsole hergestellt wurde.
5. Überprüfen Sie den Verbindungsstatus.

   Die Aktualisierung der Remote Manager Web-Konsole mit neuen Hosted Email Security Daten kann bis zu drei Stunden dauern. Hosted Email Security Kundeninformationen werden einmal pro Tag aktualisiert. Siehe *Hosted Email Security Einstellungen und Daten-Updates auf Seite 3-37*.

Einen Hosted Email Security-Kunden von der Remote Manager Web-Konsole trennen

So trennen Sie Hosted Email Security von der Remote Manager Web-Konsole:

- Wenn das Konto in die Licensing Management Platform integriert wurde, kann der Reseller das Leistungspaket aus der Licensing Management Platform-Web-Konsole löschen. Sobald das Leistungspaket gelöscht wurde, wird der Kunde von der Remote Manager Web-Konsole getrennt.
- Bei anderen Konten kann der Kunde den Remote Manager Bildschirm in der Hosted Email Security-Web-Konsole öffnen und auf **Trennen** klicken.

Der Kunde wird dann in der Hosted Email Security-Konsole benachrichtigt und klickt auf **OK**.

Produkte anderer Hersteller in Trend Micro Remote Manager integrieren

Sie können Produkte anderer Hersteller für Trend Micro Remote Manager registrieren. Weitere Informationen zu Trend Micro Produkten finden Sie unter *Trend Micro Produkte bei Trend Micro Remote Manager registrieren auf Seite 4-8*.

Integration von Autotask™

Konfigurieren Sie die folgenden Einstellungen, umAutotask™ in Remote Manager zu integrieren:

Autotask Einstellungen in Remote Manager konfigurieren

Prozedur

1. Klicken Sie auf **Administration** > **Integration anderer Anbieter konfigurieren**.

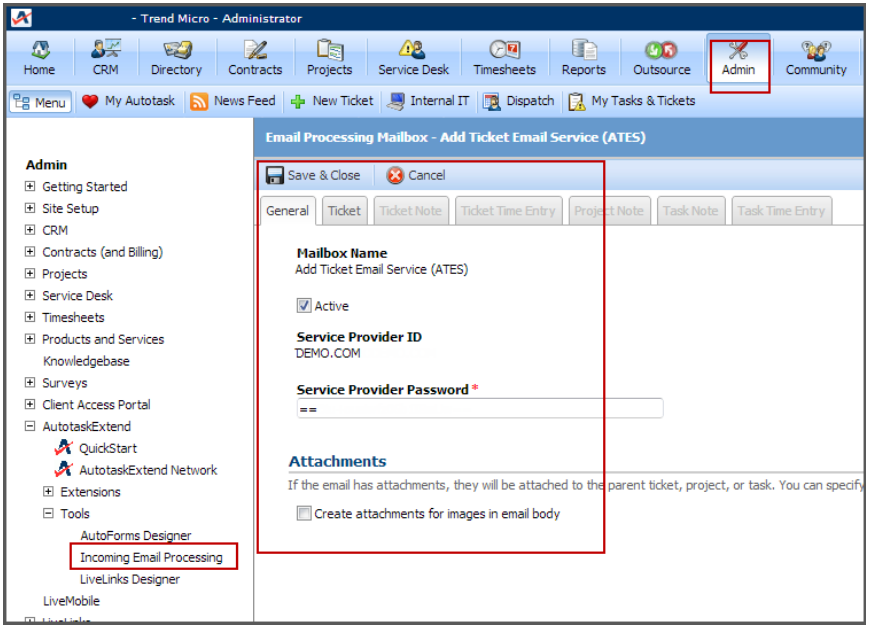
   Das Fenster **Integration anderer Anbieter** wird geöffnet.

ABBILDUNG 4-4. Gruppenfeld "Benachrichtigungen über Kontoinformationen"

2. Klicken Sie auf **Integration aktivieren**.

3. Geben Sie die Anmeldeinformationen an. Sie können die Autotask-Anmeldeinformationen unter **Admin** > **AutotaskExtend** > **Tools (Extras)** > **Incoming Email Processing (Verarbeitung eingehender E-Mails)** > **Add**

Ticket E-mail Service (ATES) (Ticket-E-Mail-Service (ATES) hinzufügen) > Edit (Bearbeiten) > General (Allgemein) überprüfen.



4. Wählen Sie die bevorzugte Sprache aus.

5. Klicken Sie auf **Speichern**.

6. Klicken Sie auf die **Customers (Kunden) > All Customers (on the tree) (Alle Kunden (in der Struktur)) > {Kunde} > Notifications (tab) (Benachrichtigungen (Registerkarte))**.

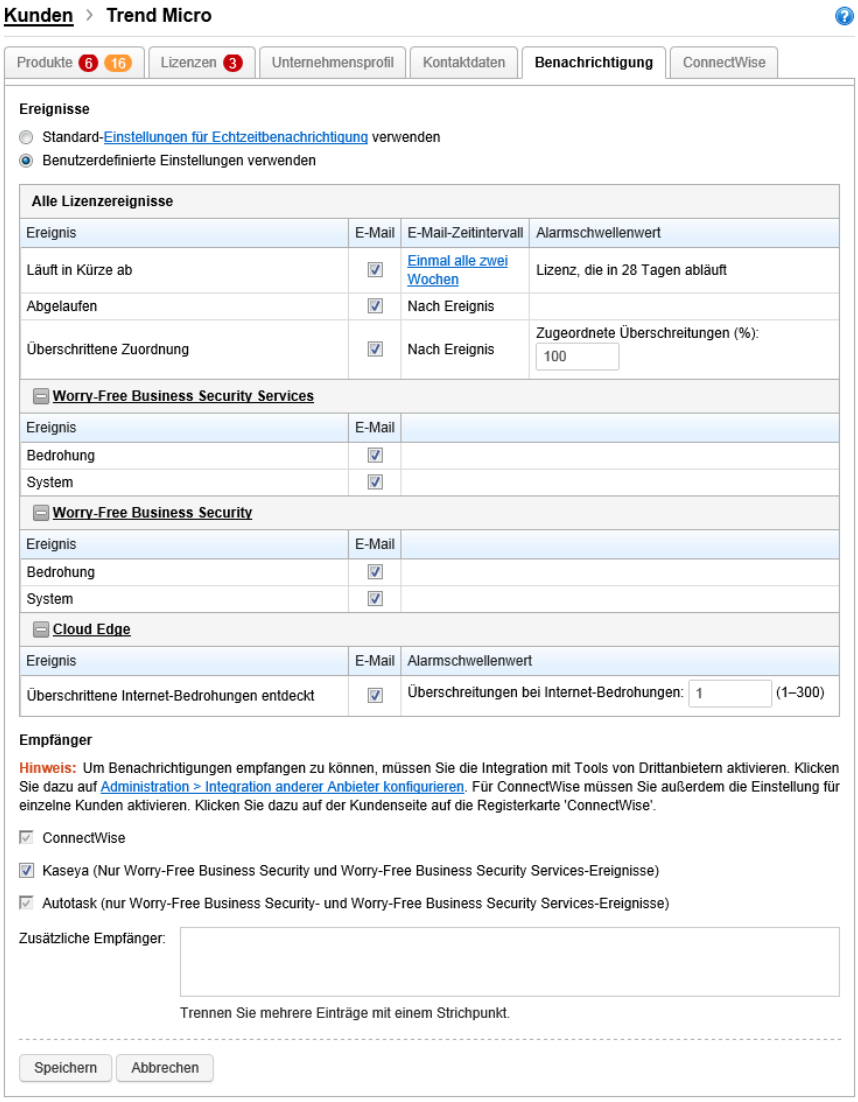


ABBILDUNG 4-5. Erforderliche Benachrichtigungen auswählen

7. Wählen Sie die Benachrichtigungen aus, die an Autotask für Worry-Free Business Security Services gesendet werden sollen.
8. Wählen Sie Autotask als einen der Empfänger aus.
9. Wiederholen Sie die Schritte 5, 6 und 7 für jeden Kunden.

Einstellungen in Autotask konfigurieren

Prozedur

1. Wechseln Sie in Autotask zu **Admin (Admin)** > **Service Desk (Servicedesk)** > **Issue and Sub-Issue Types (Problemarten und -unterarten)** > **Managed Services Alert (Alarm zu verwalteten Services)**, um die folgenden Felder zum Ticketsystem hinzuzufügen. Dadurch werden in Autotask Trend Micro Remote Manager-Benachrichtigungen angezeigt. Wählen Sie aus den folgenden Alarmtypen für verwaltete Services aus:
   - Trend Micro Bedrohungsereignisse
   - Trend Micro Systemereignisse
   - Trend Micro Lizenzereignisse

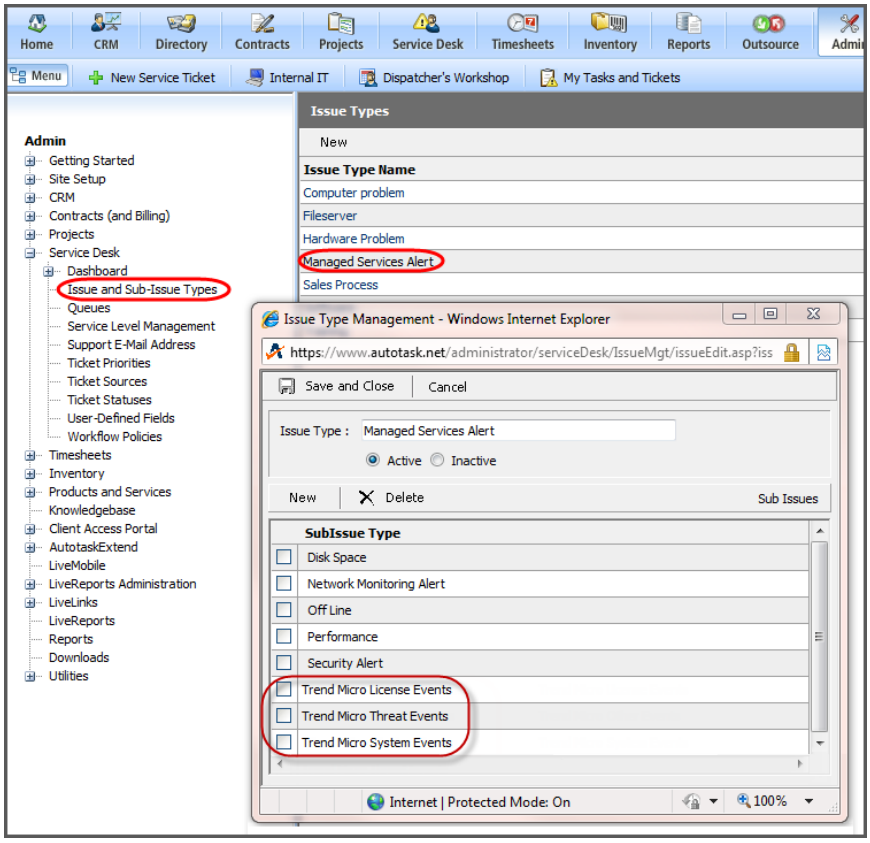
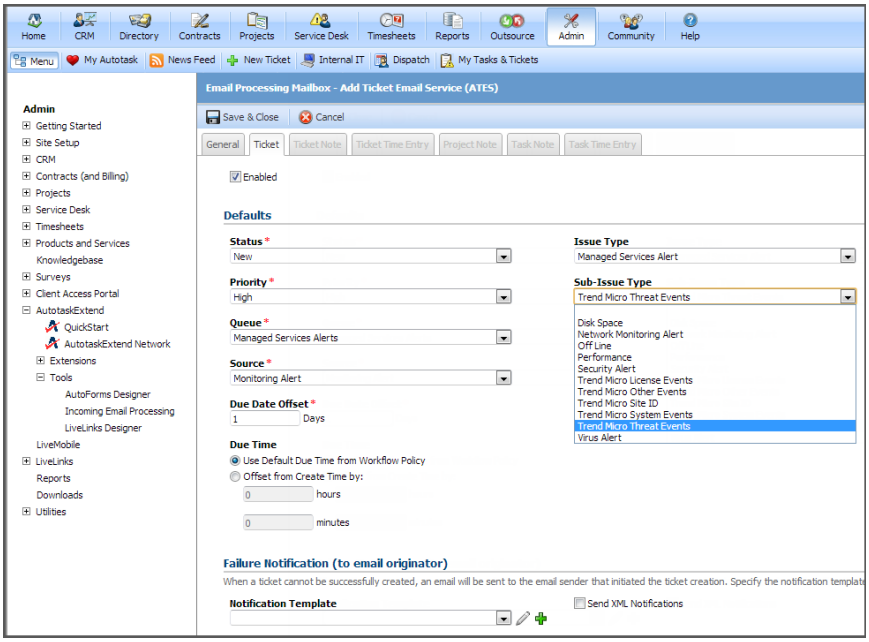


ABBILDUNG 4-6. Trend Micro Problemunterarten

2. Navigieren Sie zu **Admin** > **AutotaskExtend** > **Tools (Extras)** > **Incoming Email Processing (Verarbeitung eingehender E-Mails)** > **Add Ticket E-mail Service (ATES) (Ticket-E-Mail-Service (ATES) hinzufügen)** > **Edit (Bearbeiten)** > **Ticket** und stellen Sie sicher, dass die E-Mail-Einstellung richtig ist:



3. Navigieren Sie zu **Admin** > **Site Setup (Website-Setup)** > **User-Defined Fields (Benutzerdefinierte Felder)** und erstellen Sie das Feld "Trend Micro Site ID":

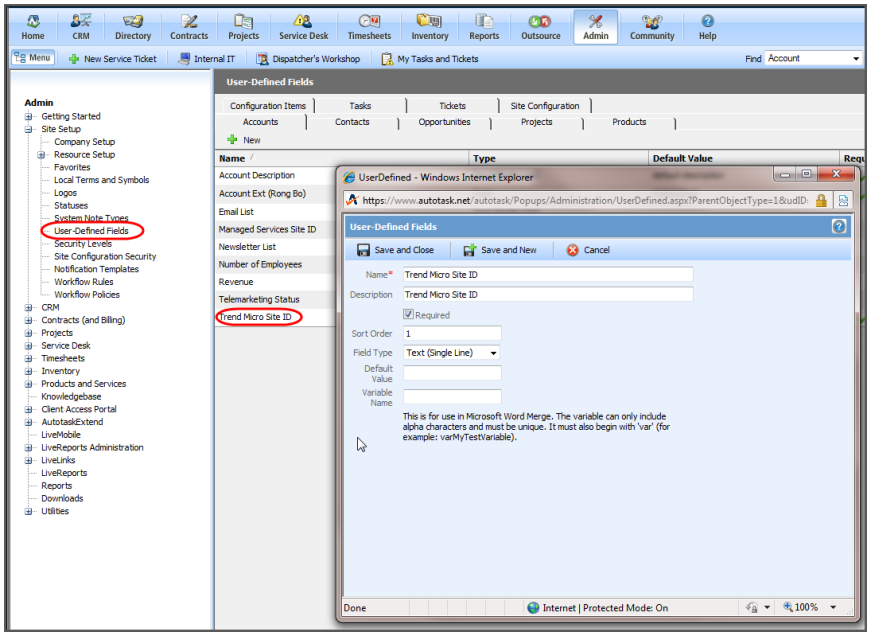
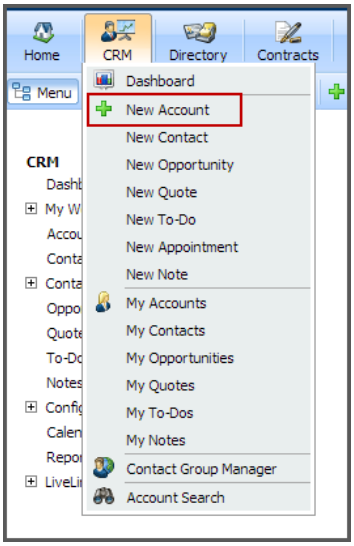


ABBILDUNG 4-7. Trend Micro Site ID Definition

4. Gehen Sie zu **CRM** > **New Account (Neues Konto)** und geben Sie die eindeutige Remote Manager ID in das neue Feld "Trend Micro Site ID" ein.

   Dies ist die von Remote Manager exportierte eindeutige ID.



Integration von Kaseya™

Konfigurieren Sie die folgenden Einstellungen, um Kaseya™ in Remote Manager zu integrieren:

Kaseya-Einstellungen in Remote Manager konfigurieren

Prozedur

1. Klicken Sie auf **Administration** > **Integration anderer Anbieter konfigurieren**.

Das Fenster **Integration anderer Anbieter** wird geöffnet.

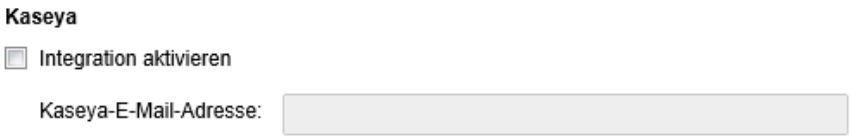


ABBILDUNG 4-8. GRUPPENFELD "BENACHRICHTIGUNGEN ÜBER KONTOINFORMATIONEN"

2. Klicken Sie auf **Integration aktivieren**.
3. Fügen Sie die Kaseya-E-Mail-Adresse hinzu.
4. Klicken Sie auf **Speichern**.
5. Navigieren Sie zu **Customers (Kunden) > All Customers (on the tree) (Alle Kunden (in der Struktur)) > {Kunde} > Notifications (tab) (Benachrichtigungen (Registerkarte))**.

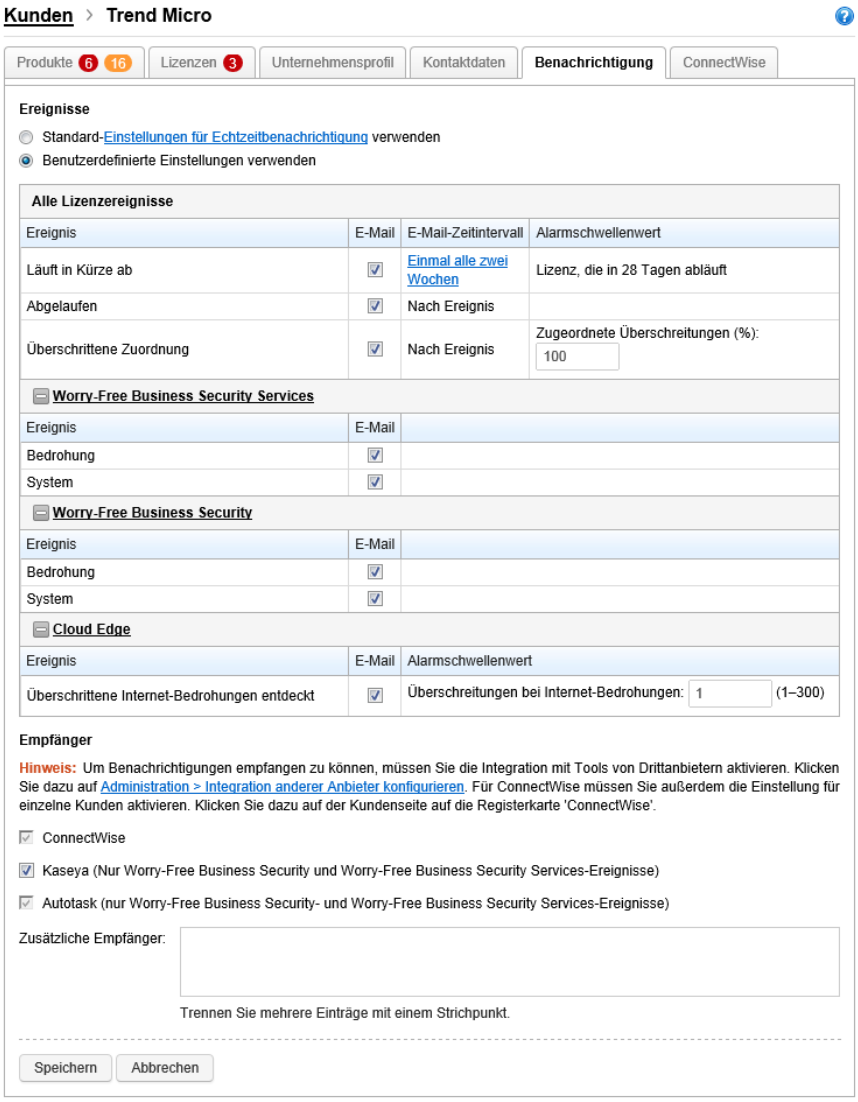


ABBILDUNG 4-9. Erforderliche Benachrichtigungen auswählen

6. Wählen Sie die Produktbenachrichtigungen aus, die an Kaseya gesendet werden sollen.

> **Hinweis**
>
> Sie wählen die Standardeinstellung für Echtzeitbenachrichtigungen aus, die auf alle Produkte und Kunden angewendet werden können. Alternativ können Sie die Einstellungen für diesen Kunden angeben.

7. Wählen Sie Kaseya als einen der Empfänger aus.

8. Wiederholen Sie die Schritte 5, 6 und 7 für jeden Kunden.

Einstellungen in Kaseya konfigurieren

Prozedur

1. Fügen Sie in Kaseya die folgenden Felder zum Ticketsystem hinzu, um Trend Micro Remote Manager Benachrichtigungen anzuzeigen.

   - Worry-Free Business Security

Feldname	Zweck
TM_CreateTime	Ereigniserstellungszeit
TM_ProductName	Produktname
TM_AgentGUID	Remote Manager Agent-GUID
TM_CustomerName	Kunde/Firmenname
TM_EventName	Ereignisname
TM_ServerName	Client Server Messaging/Worry-Free Business Security-Servername
TM_MASClientName (optional)	Namen des Exchange Servers (betrifft nur das Ereignis "Exchange Server herunterfahren")

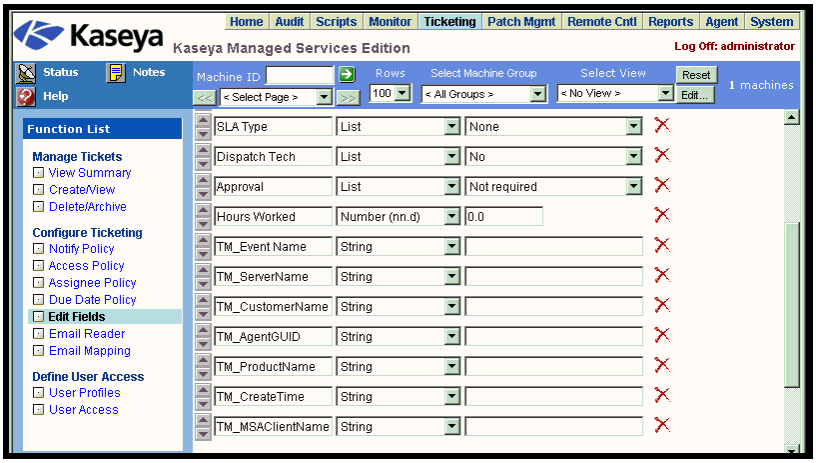


ABBILDUNG 4-10. Kaseya Ticketfelder

- Worry-Free Business Security Services

FELDNAME	ZWECK
TM_CreateTime	Ereigniserstellungszeit
TM_ProductName	Produktname
TM_CustomerName	Kunde/Firmenname
TM_EventName	Ereignisname

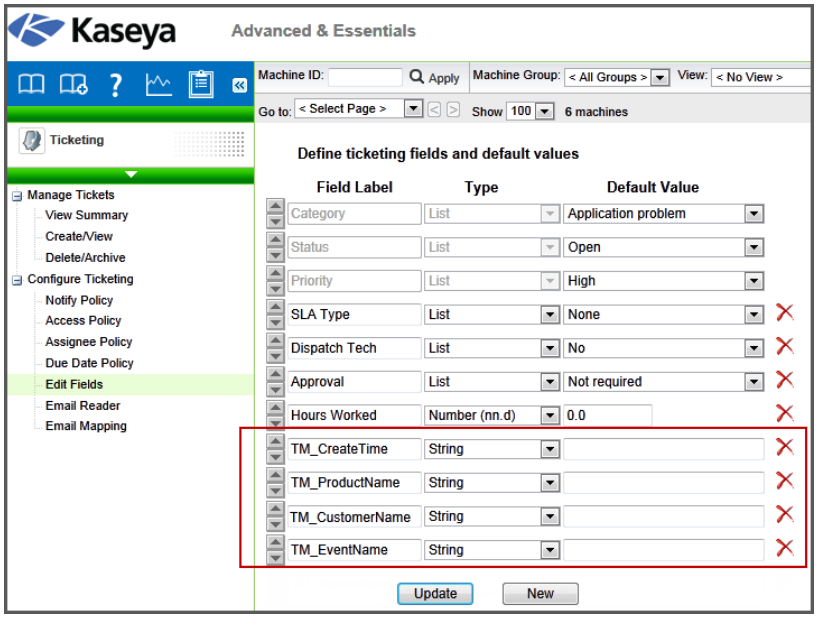


ABBILDUNG 4-11. Kaseya Ticketfelder

2. Stellen Sie sicher, dass die E-Mail-Einstellung der Einstellung im folgenden Fenster entspricht:

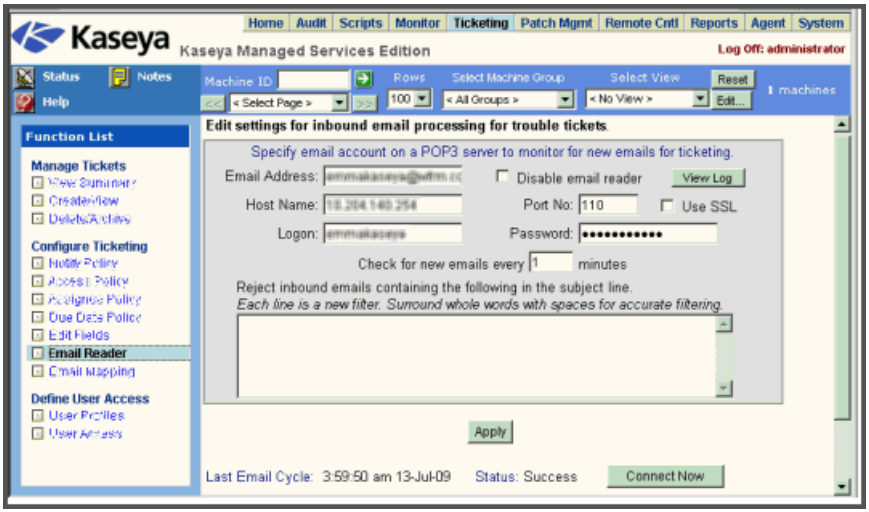


ABBILDUNG 4-12. Kaseya E-Mail-Einstellungen

Wenn ein Ereignis ausgelöst wird, erhält Kaseya das Ticket:

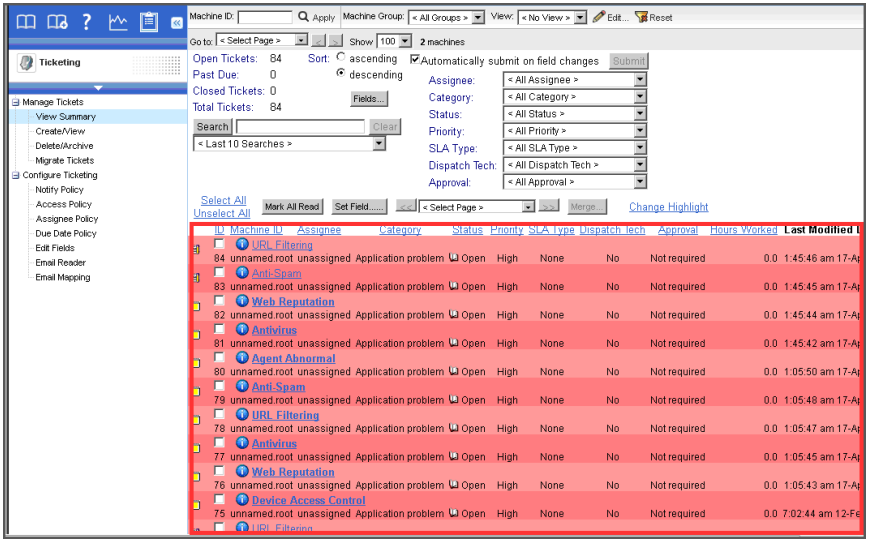


ABBILDUNG 4-13. Kaseya Ereignis-Ticket

Integration von ConnectWise™

Konfigurieren Sie die folgenden Einstellungen, um ConnectWise™ mit Remote Manager zu integrieren:

Allgemeine ConnectWise Einstellungen in Remote Manager konfigurieren

Prozedur

1. Gehen Sie zu **Administration** > **Integration anderer Anbieter konfigurieren**.

Das Fenster **Integration anderer Anbieter** wird geöffnet.

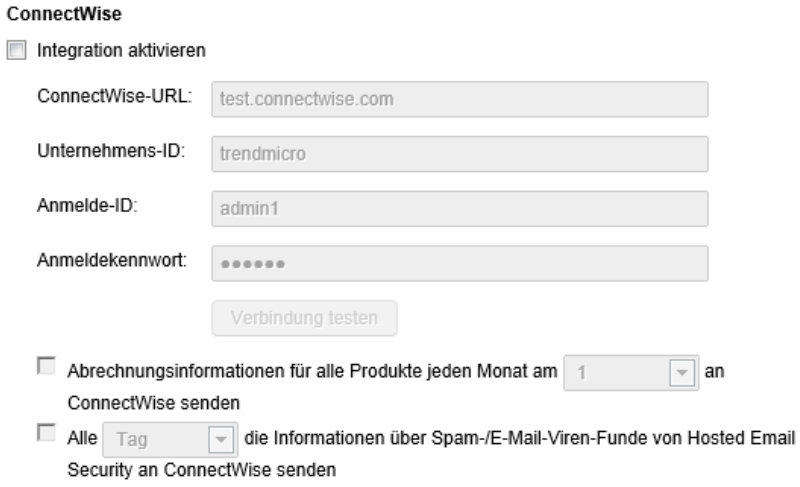


ABBILDUNG 4-14. Gruppenfeld "Benachrichtigungen über Kontoinformationen"

2. Aktualisieren Sie Folgendes:

   - **ConnectWise-Integration aktivieren**: Aktivieren Sie das Kontrollkästchen, um die Integration zwischen Trend Micro Remote Manager und ConnectWise zu aktivieren.
   - **ConnectWise-URL**: Geben Sie den URL des Services ein.
   - **Unternehmens-ID**
   - **Anmelde-ID**: Das Konto, das zur Anmeldung bei ConnectWise verwendet wird.
   - **Anmeldekennwort**: Das dem Konto zugewiesene Kennwort.
   - Wählen Sie, wie oft Remote Manager Abrechnungsinformationen senden soll.
   - Wählen Sie, wie oft Remote Manager Spam-Statistiken senden soll.

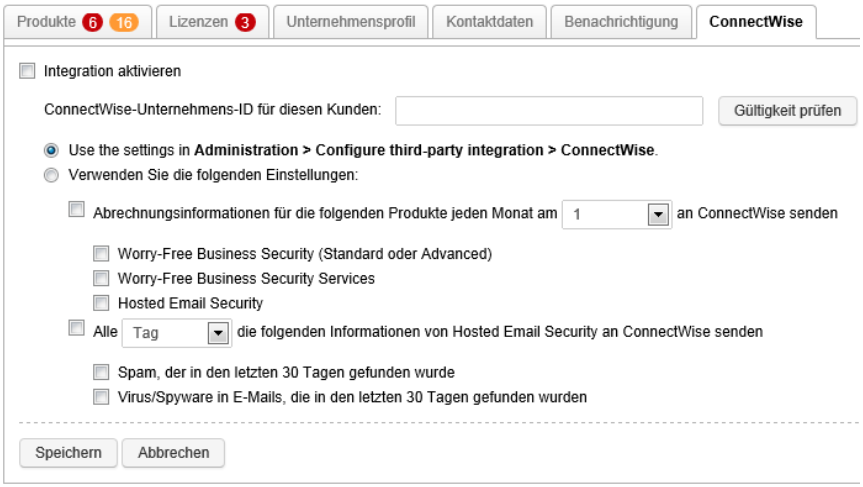
3. Klicken Sie auf **Speichern**.

Kundenspezifische ConnectWise-Einstellungen in Remote Manager konfigurieren

Konfigurieren Sie die ConnectWise-Einstellungen für jeden Kunden. Diese Einstellungen sind optional. Wenn Sie jedoch auch kundenspezifische Benachrichtigungen erhalten möchten, müssen Sie diese Funktion aktivieren.

Prozedur

1. Wechseln Sie zu **Kunden (Registerkarte)** > **{Kunde}** > **ConnectWise (Registerkarte, rechter Fensterbereich)**.


Produkte 6 16
Lizenzen 3
Unternehmensprofil
Kontaktdaten
Benachrichtigung
ConnectWise
Integration aktivieren
ConnectWise-Unternehmens-ID für diesen Kunden:
Gültigkeit prüfen
Use the settings in Administration > Configure third-party integration > ConnectWise.
Verwenden Sie die folgenden Einstellungen:
Abrechnungsinformationen für die folgenden Produkte jeden Monat am 1 an ConnectWise senden
Worry-Free Business Security (Standard oder Advanced)
Worry-Free Business Security Services
Hosted Email Security
Alle Tag die folgenden Informationen von Hosted Email Security an ConnectWise senden
Spam, der in den letzten 30 Tagen gefunden wurde
Virus/Spyware in E-Mails, die in den letzten 30 Tagen gefunden wurden
Speichern
Abbrechen

2. Wählen Sie **Integration aktivieren** aus.
3. Geben Sie eine gültige in ConnectWise vorhandene **Unternehmens-ID** an.

> **Hinweis**
>
> Sie können auf **Gültigkeit prüfen** klicken, um die Unternehmens-ID zu prüfen, wenn Sie sich bezüglich der Schreibweise nicht sicher sind.

4. Wählen Sie die Integrationseinstellungen.

- Verwenden Sie die Standardeinstellungen unter **Administration**.
- Geben Sie Ihre eigenen Optionen für die Abrechnung und Zusammenfassungen für Führungskräfte an.

5. Klicken Sie auf **Speichern**.
6. Wechseln Sie zu **Kunden (Registerkarte)** > **{Kunde}** > **Benachrichtigung (Registerkarte, rechter Fensterbereich)**.
7. Konfigurieren Sie die Benachrichtigungseinstellungen für diesen Kunden.
8. Wählen Sie **ConnectWise** als einen der Empfänger aus.
9. Klicken Sie auf **Speichern**.

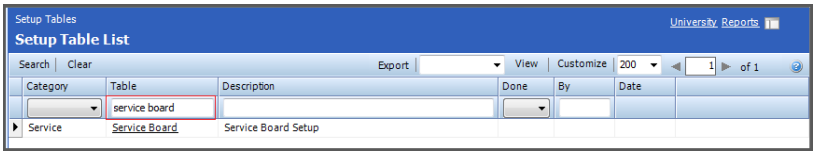
Einstellungen in ConnectWise konfigurieren

Prozedur

1. Melden Sie sich bei ConnectWise mit dem Professional Services Automation (PSA) Tool an.
2. Erstellen Sie ein neues Service-Board.

   Dies ist ein optionaler Schritt. Die Ausführung dieses Schrittes hilft Ihnen jedoch, Ergebnisse aus Trend Micro Remote Manager effizient zu filtern.

   a. Wechseln Sie zu **Setup** > **Setup Table (Setup-Tabelle)** > **Suchen** und geben Sie `Service Board` ein.



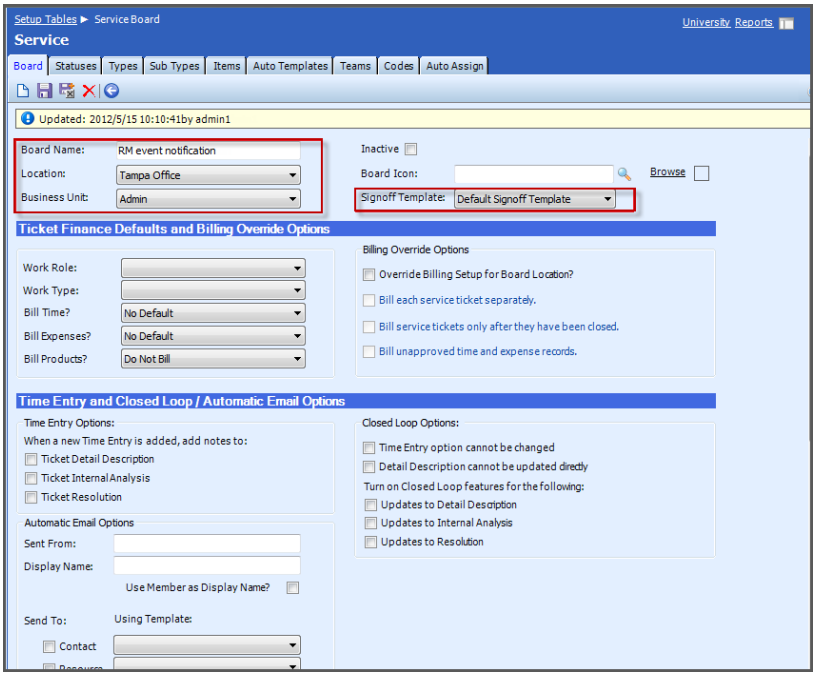
   b. Klicken Sie auf **Service Board (Service-Board)**.

      Eine Liste von Service-Boards wird angezeigt.

   c. Klicken Sie auf das Symbol Neu, um ein neues Service-Board zu erstellen.

Das Fenster New Service Board (Neues Service-Board) wird angezeigt.

d. Aktualisieren Sie **Board Name (Boardname)**, **Location (Standort)**, **Business Unit (Geschäftsstelle)** und **Sign Off Template (Freigabevorlage)**. Alle anderen Felder sind optional.



e. Klicken Sie auf **Speichern**.

f. Klicken Sie auf die Registerkarte **Statuses (Statuswerte)**.

g. Klicken Sie auf das Symbol Neu, um einen neuen Status-Service zu erstellen.

h. Aktualisieren Sie **Status to Description (Status nach Beschreibung)**, **Sort Order (Sortierreihenfolge)** und markieren Sie **Display on Board (In Board anzeigen)**.

i. Klicken Sie auf **Speichern**.

3. Weisen Sie dem Benutzer Berechtigungen zu.

a. Wechseln Sie zu **Setup** > **Setup Table (Setup-Tabelle)** > **Suchen** und geben Sie `Integrator Login` ein.

b. Klicken Sie auf den erforderlichen Link **Integrator Login** (Integrator-Anmeldung) und klicken Sie anschließend auf das neue Symbol, um ein neues Konto zur Anmeldung zu erstellen.

   Das Fenster **Allgemein** wird angezeigt.

c. Wählen Sie unter **Access Levels** (Zugriffsebene) **All records** (Alle Datensätze) aus.

d. Markieren Sie die folgenden Optionen: **Service Ticket API (Serviceticket-API)**, **Management Services API (Verwaltungsdienste-API)**, **Company API (Firmen-API)**, **System API (System-API)** und **Configuration API (Konfigurations-API)**.

e. Wählen Sie das zuvor von Ihnen erstellte Service-Board aus, aktualisieren Sie die **Ticket-Callback-URL** auf `www.example.com` oder eine andere beliebige URL und klicken Sie dann auf **Speichern**.

f. Klicken Sie auf **Speichern**.

4. Erstellen Sie eine neue Verwaltungslösung.

   a. Wechseln Sie zu **Setup** > **Setup Table (Setup-Tabelle)** > **Suchen** und geben Sie `Management IT` ein.

   b. Klicken Sie auf **Management IT (Verwaltungs-IT)**.

   c. Klicken Sie auf das Symbol Neu, um eine neue Verwaltungslösung zu erstellen.

   d. Aktualisieren Sie **Name** auf `TMRM Management Setup`, **Verwaltungs-IT-Lösung** auf `Custom` und **Name der benutzerdefinierten Lösung** auf `TMRM Management Solution`.

      Bei Verwendung von anderen Werten kann die Verbindung unterbrochen werden.

   e. Klicken Sie auf **Speichern**.

5. Ändern Sie den Standardstatus der Firma zu `Active (Aktiv)`.

a. Wechseln Sie zu **Setup** > **Setup Table (Setup-Tabelle)** > **Suchen** und geben Sie `Company Status` ein.

b. Klicken Sie auf **Company Status (Firmenstatus)**.

c. Klicken Sie auf **Active (Aktiv)**.

d. Wählen Sie **Default Flag (Standard-Flag)**.

e. Klicken Sie auf **Speichern**.

6. Erstellen Sie jeweils einen neuen Service für alle von Remote Manager verwalteten Produkte/Services.

a. Navigieren Sie zu **Setup** > **Products (Produkte)** > **New (Neu)**.

b. Aktualisieren Sie die **Produkt-ID** auf ein verwaltetes Produkt/einen verwalteten Service. Wählen Sie zwischen `HES/WFBS-SVC/WFBS-S/WFBS-A`.

c. Aktualisieren Sie den Preis nach Bedarf.

d. Klicken Sie auf **Speichern**.

Wiederholen Sie diese Schritte für alle verwalteten Produkte/Services.

7. Erstellen Sie Querverweise für alle von Remote Manager verwalteten Produkte/Services.

a. Navigieren Sie zu **Setup** > **Setup Table (Setup-Tabelle)** > **Suchen** und geben Sie `Managed Devices Integration` ein.

b. Klicken Sie auf **Managed Devices Integration** (Integration verwalteter Geräte).

c. Wählen Sie die Verwaltungslösung mit der Bezeichnung "**Remote Manager Verwaltungslösung**".

d. Navigieren Sie zur Registerkarte **Cross Reference (Querverweis)** > **New (Neu)**.

e. Aktualisieren Sie die Felder nach Bedarf.

Einstellungen für von Remote Manager verwaltete Produkte/Services.

PRODUKT/SERVICE	EINSTELLUNGEN
Worry-Free Business Security Standard	• **Typ**: `T-WFBS-S` • **Stufe**: `Standard` • **Agreement Type (Vertragstyp)**: `Managed Service` • **Produkt**: `WFBS-S` • **Configuration Type (Konfigurationstyp)**: `Spam Stats`
Worry-Free Business Security Advanced	• **Typ**: `T-WFBS-A` • **Stufe**: `Advanced` • **Agreement Type (Vertragstyp)**: `Managed Service` • **Produkt**: `WFBS-A` • **Configuration Type (Konfigurationstyp)**: `Spam Stats`
Worry-Free Business Security Services	• **Typ**: `T-WFBSS` • **Stufe**: `Standard` • **Agreement Type (Vertragstyp)**: `Managed Service` • **Produkt**: `WFBSS` • **Configuration Type (Konfigurationstyp)**: `Spam Stats`
Hosted Email Security	• **Typ**: `T-HES` • **Stufe**: `Standard` • **Agreement Type (Vertragstyp)**: `Managed Service` • **Produkt**: `HES` • **Configuration Type (Konfigurationstyp)**: `Spam Stats`

f. Klicken Sie auf **Speichern**.

8. Erstellen Sie eine neue Firma für jeden Kunden, den Sie in ConnectWise integrieren möchten.

   a. Wechseln Sie zu **Kontakte** > **Firma** > **Neu**.

   b. Aktualisieren Sie **Unternehmens-ID**.

      Trend Micro empfiehlt, den Remote Manager Kundennamen als ConnectWise Unternehmens-ID zu verwenden.

   c. Klicken Sie auf **Speichern**.

      Wiederholen Sie diese Schritte, um eine Firma für jeden Kunden zu erstellen.

9. Erstellen Sie eine neue Verwaltung für jede Firma.

   a. Klicken Sie auf die Registerkarte **Management** (Verwaltung).

   b. Klicken Sie auf **Speichern**.

   c. Klicken Sie auf **New Item** (Neues Element).

   d. Aktualisieren Sie die Angabe unter **Lösung** auf `Remote Manager Management Solution`.

   e. Aktualisieren Sie die **Managed ID** (Verwaltungs-ID) auf die im vorherigen Schritt angegebene Unternehmens-ID.

   f. Klicken Sie auf **Speichern**.

10. Erstellen Sie Konfigurationen für jede Firma.

    a. Klicken Sie auf die Registerkarte **Configuration**.

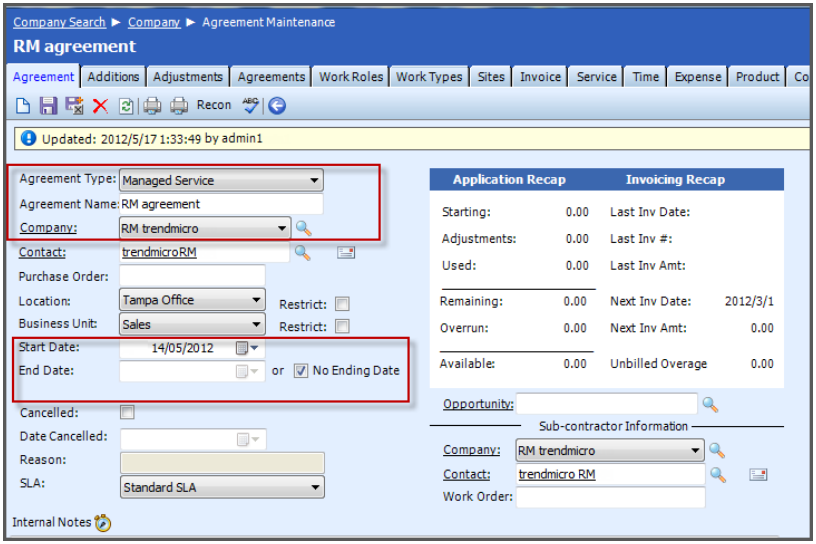
    b. Erstellen Sie eine neue Konfiguration und setzen Sie **Konfigurationstyp** auf `Spam Stats` sowie **Name** auf die Unternehmens-ID.

    c. Klicken Sie auf **Speichern**.

11. Erstellen Sie einen neuen Vertrag für jeden Kunden, den Sie in ConnectWise integrieren möchten.

    a. Navigieren Sie zur Registerkarte **Verträge** > **Neu**.

b. Wählen Sie `Managed Service` als **Vertragstyp** und aktualisieren Sie die anderen Daten nach Bedarf.



c. Klicken Sie auf **Speichern**.

12. Fügen Sie Zusätze zum Vertrag ebenfalls hinzu.

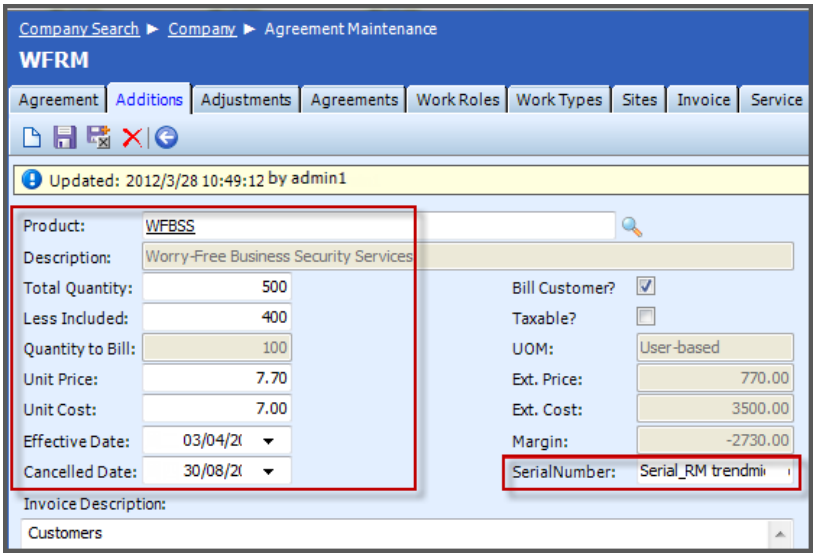
a. Wechseln Sie zu **Agreements (Verträge)** > **Additions (Zusätze)**.

b. Aktualisieren Sie die Felder nach Bedarf.

Aktualisieren Sie z. B. den Preis und die Seriennummer.

Wichtig

Die Seriennummer muss im Format `SerialNumber: Serial_Company ID` eingegeben werden.



c. Klicken Sie auf **Speichern**.

Wiederholen Sie diese Schritte für alle verwalteten Produkte/Services.

Kapitel 5

Kunden verwalten

Dieser Abschnitt enthält das folgende Thema:

- *Kunden auf Seite 5-2*

Kunden

Überprüfen Sie die Kundendaten und Lizenzinformationen über die Seite **Kunden**. Sie können auch Folgendes tun:

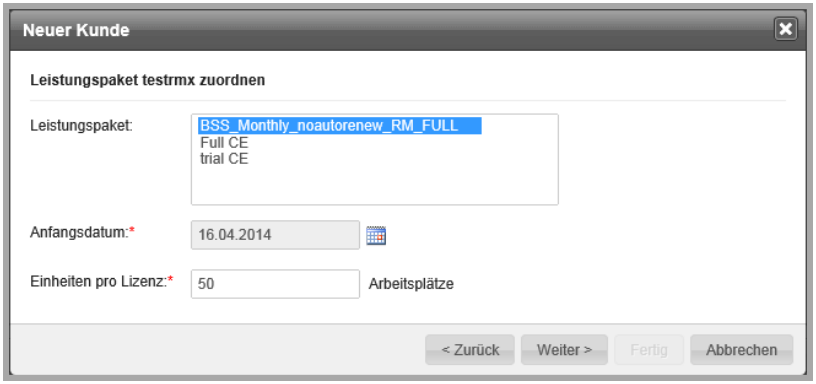
- Auf die Namen der einzelnen Kunden klicken, um weitere Kundeninformationsdetails anzuzeigen
- Die Kundenliste filtern
- Die Kundeninformationen in eine `csv`-Datei exportieren
- Hinzufügen neuer Kunden
- Lizenzen verlängern
- Produkte verwalten

Neue Kunden hinzufügen

Prozedur

- Bei Licensing Management Platform-Konten:

  1. Navigieren Sie zu **Kunden** > **{Kundenname}** > **Produkte (Registerkarte)** > **Hinzufügen**.



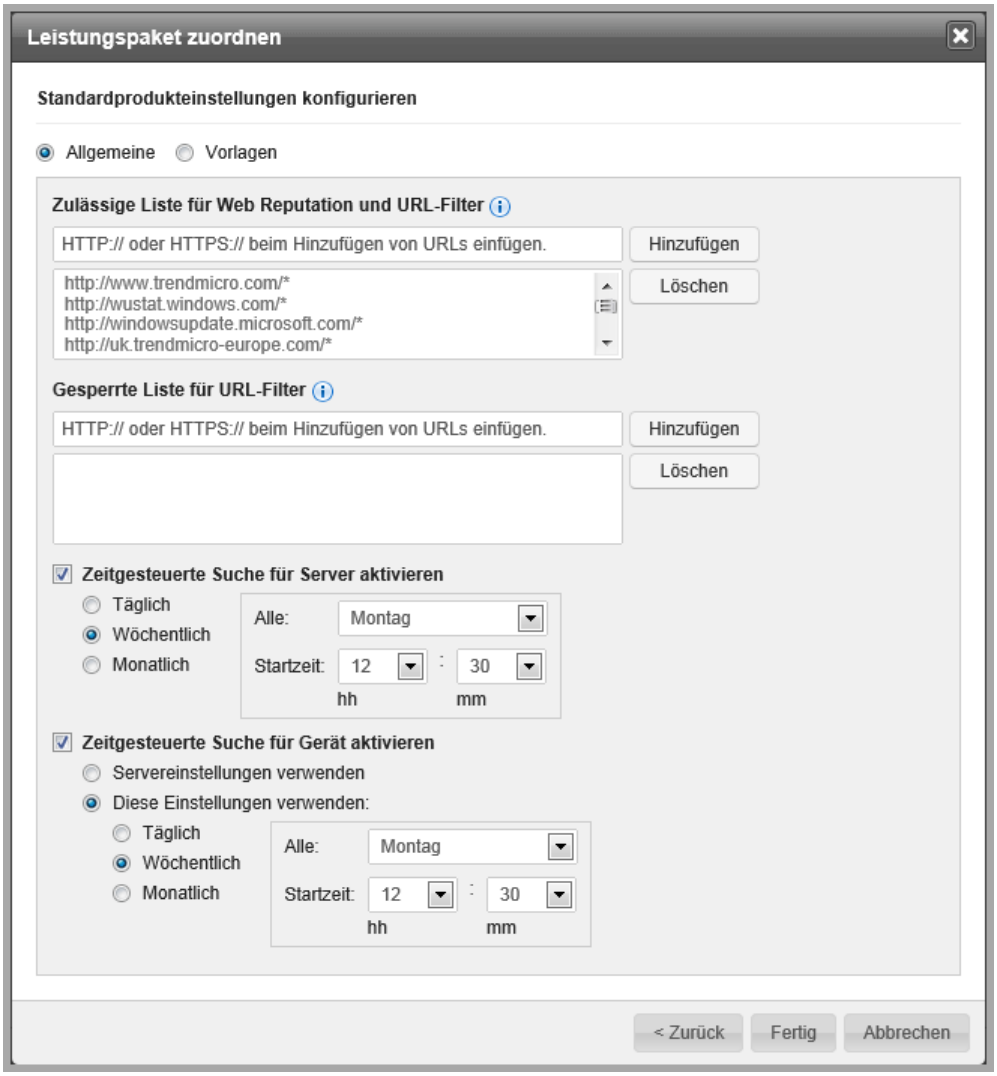
2. Wählen Sie das Leistungspaket, das Anfangsdatum und die Anzahl der Einheiten pro Lizenz aus.

3. Klicken Sie auf **Weiter**.

4. Konfigurieren Sie die Standardeinstellungen für das Produkt. Sie können aus folgenden Einstellungen auswählen:

Hinweis

Diese Funktion wird nur angezeigt, wenn Sie Worry-Free Business Security Services ausgewählt haben.



- **Allgemein**: Konfigurieren Sie nur die angezeigten Einstellungen.
  - Zulässige Liste für Web Reputation und URL-Filter

Hinweis

Wenn Sie der Zulässigen Liste eine URL hinzufügen, stellen Sie sicher, dass diese URL nicht der Liste der gesperrten URLs hinzugefügt wurde, und umgekehrt.

- Gesperrte Liste für URL-Filter
- Zeitgesteuerte Suche für Server und Gerät

- **Vorlagen**: Navigieren Sie zu **Administration** > **Standardeinstellungsvorlagen konfigurieren**, um weitere Einstellungen unter Verwendung einer Konsole einzurichten, die Worry-Free Business Security ähnelt.

5. Klicken Sie auf **Fertig**.

   Das Produkt/der Service werden hinzugefügt und die Details der Hinzufügung werden angezeigt.

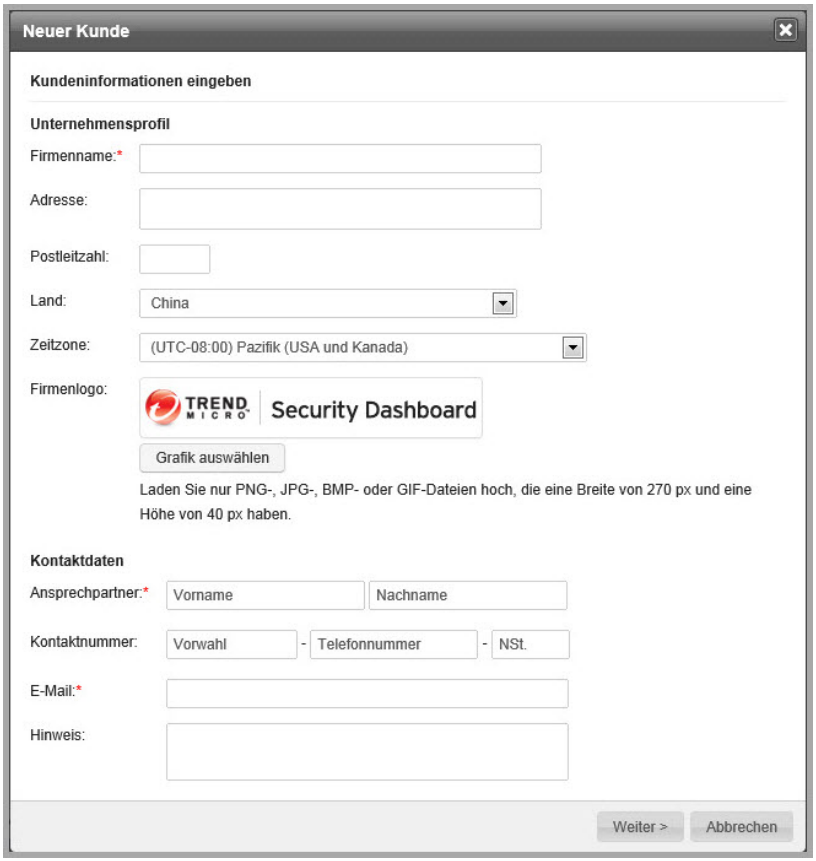
Hinweis

Notieren Sie sich die GUID oder den Autorisierungsschlüssel.

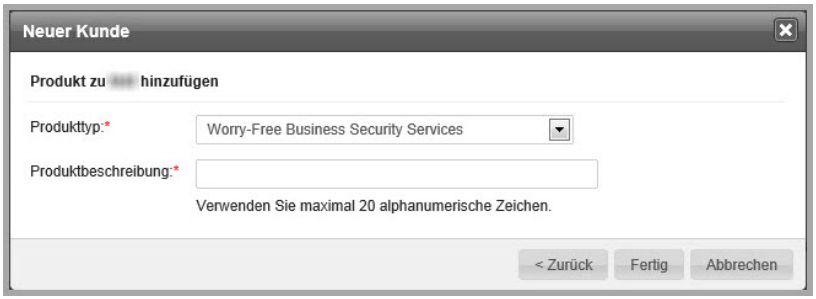
6. Klicken Sie auf **Connect (Verbinden)**, um Informationen zum Verbinden des Produkts/Services mit der Konsole zu erhalten.

- Bei anderen Konten:

1. Klicken Sie im Banner auf **Neuer Kunde** oder wechseln Sie zu **Kunden** > **Neuer Kunde**. Es wird eine Seite Neuer Kunde geöffnet.



2. Geben Sie die erforderlichen Informationen an.
3. Klicken Sie auf **Weiter >**.
4. Wählen Sie den Produkttyp aus und geben Sie eine Produktbeschreibung an.



5. Klicken Sie auf **Fertig**.

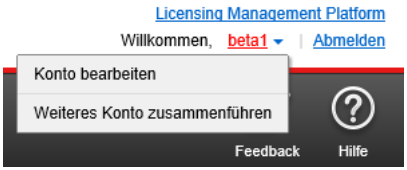
Konten zuweisen

Wenn Sie andere Trend Micro Remote Manager Konten verwalten, die nicht auf die neue Licensing Management Platform migriert wurden, können Sie diese Konten mit dem aktuellen Konto zusammenführen.

Prozedur

1. Melden Sie sich bei einem Remote Manager Konto an, das in die Licensing Management Platform migriert wurde.

   Das Fenster **Dashboard** wird angezeigt.



2. Klicken Sie auf den Pfeil neben dem Anmeldenamen und klicken Sie auf **Weiteres Konto zusammenführen** > **Weiter**.

Warnung!

Wenn Sie ein Konto mit dem aktuellen Konto zusammenführen, werden alle Daten des anderes Kontos verschoben. Wenn Sie beispielsweise derzeit als `admin1` angemeldet sind und Sie das Konto `admin2` mit dem Konto`admin1` zusammenführen, werden alle Daten von `admin2` aus dem Konto `admin2` gelöscht. Diese Daten werden mit dem Konto `admin1` zusammengeführt. Sie können das Konto `admin2` zwar weiterhin öffnen, es befinden sich jedoch sämtliche Daten im Konto `admin1`.

3. Geben Sie den Benutzernamen und das Kennwort des Kontos an, das Sie mit dem aktuellen Konto zusammenführen möchten.

4. Klicken Sie auf **Zusammenführung**.

   Warten Sie einen Moment, bis die Zusammenführung der Daten abgeschlossen ist.

Nächste Maßnahme

Nach der Migration des Kontos wird beim Hinzufügen eines neuen Kunden immer Folgendes angezeigt:

- **Mit einem aktiven Licensing Management Platform-Konto**: Wenn der neue Kunde bereits ein Konto in der Licensing Management Platform besitzt.
- **Mit vorhandenen Produktservern, die mit diesem Konto verbunden werden müssen**: Wenn der Kunde ein Produkt/einen Service besitzt, aber das Konto noch nicht in die Licensing Management Platform integriert wurde.

Produktlizenz überprüfen

Überprüfen Sie die Produktlizenzen auf den verwalteten Servern Ihrer Kunden regelmäßig, um permanenten Schutz zu gewährleisten.

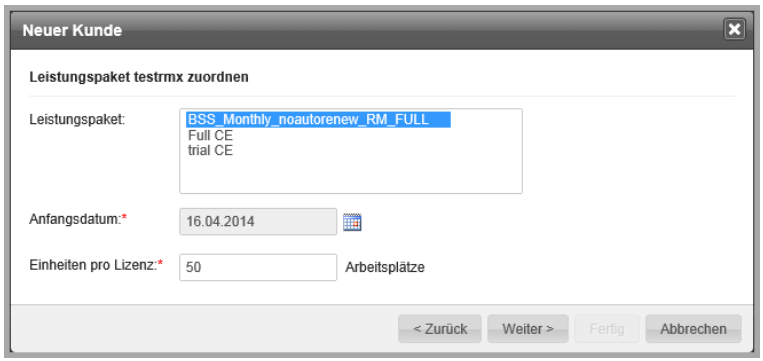
Prozedur

1. Klicken Sie auf **Kunden** > **{Kunde}** > **{Produkt}** > **Lizenz (Registerkarte)**.
2. Überprüfen Sie die Informationen zur Produktlizenz.

Produkte/Services hinzufügen

Prozedur

1. Navigieren Sie zu **Kunden** > **{Kundenname}** > **Produkte (Registerkarte)** > **Hinzufügen**.
   - Bei Licensing Management Platform-Konten:
     a. Wählen Sie das Leistungspaket, das Anfangsdatum und die Anzahl der Einheiten pro Lizenz aus.



     b. Fügen Sie das Produkt oder den Service hinzu.

Das Produkt/der Service werden hinzugefügt und die Details der Hinzufügung werden angezeigt.

c. Klicken Sie auf **Fertig**.

- Wenn Sie ein Konto verwenden, dass in die Trend Micro Licensing Management Platform integriert ist:

  a. Wählen Sie den Produkttyp aus und fügen Sie eine Produktbeschreibung hinzu.

  b. Klicken Sie auf **Fertig**.

  c. Notieren Sie sich die GUID oder den Autorisierungsschlüssel. Sie benötigen dies, wenn Sie *Ihre Produkte registrieren auf Seite 4-8*.

Kontakte

Wenn Ihr Konto mit der Licensing Management Platform verknüpft ist, klicken Sie über **Abmelden** auf den Link **Licensing Management Platform**, um Ihre Kontakte zu bearbeiten.

Kundenliste filtern

Die Kundenliste kann eine kurze oder lange Liste anzeigen, je nachdem, wie viele Kunden Sie haben. Um die erforderlichen Informationen abzurufen, können Sie die Kunden eingrenzen und nur die Kunden finden, die dem festgelegten Profil entsprechen.

Prozedur

1. Klicken Sie in der Remote Manager Web-Konsole auf **Kunden**.

   Auf dieser Seite werden alle Ihre Kunden angezeigt.

2. Wählen Sie auf der rechten Seite ein oder mehrere Felder aus.

   Hinweis

   Wenn Sie mehr als ein (1) Feld auswählen, wird möglicherweise die spezifische Information, die Sie benötigen, angezeigt, und das ist gut. Es besteht jedoch auch die Möglichkeit, dass Sie die benötigte Information herausgefiltert haben. Gehen Sie daher bei der Filterauswahl sorgfältig vor.

3. (Optional) Klicken Sie auf **Exportieren**, um eine CSV-Datei zu erstellen, die Ihre gefilterten Kunden enthält.

Kapitel 6

Agents verwalten

Dieser Abschnitt enthält die folgenden Themen:

- *Agents über die Remote Manager Web-Konsole verwalten auf Seite 6-2*
- *Agents über den verwalteten Server verwalten auf Seite 6-6*
- *Agents entfernen auf Seite 6-15*

Agents über die Remote Manager Web-Konsole verwalten

Dieser Abschnitt enthält Informationen über die Verwaltung von Agents über die Trend Micro™ Remote Manager™ Web-Konsole.

Verbindung zwischen Agent und Server überprüfen

Um sicherzustellen, dass der Trend Micro Remote Manager Service ordnungsgemäß ausgeführt wird, müssen die Agents auf der Remote Manager Web-Konsole "verbunden" oder "online" sein.

Navigieren Sie zu **Kunden** > **{Kunde}** > **Produkte (Registerkarte)** .

In der Struktur wird der Status jedes Agents in der Spalte **Status** angezeigt. Details über jeden Status finden Sie unter *Agent-Status auf Seite 6-2*.

Zusätzlich zum aktuellen Kapitel finden Sie unter *Fehlerbehebung und bekannte Probleme auf Seite 11-1* weitere Erläuterungen von Problemen im Zusammenhang mit der Verbindung zwischen Server und Agent.

Agent-Status

Der Status eines Remote Manager Agents zeigt an, ob der Agent Daten sammeln und Befehle vom Remote Manager Server empfangen kann. Der Status zeigt auch den Grund an, weshalb der Agent nicht ordnungsgemäß funktioniert, und wie Sie dieses Problem beheben können. Die folgende Tabelle beschreibt die verschiedenen Agent-Statustypen und Möglichkeiten zum Beheben dieses Problems.

TABELLE 6-1. Agent-Statustypen

STATUS	BESCHREIBUNG	LÖSUNG
Online	Der Agent wird ordnungsgemäß ausgeführt.	n. v.

Status	Beschreibung	Lösung
Ungewöhnlich	Der Agent erscheint offline und antwortet nicht auf den Remote Manager Server, hat aber keine Abmeldungsanfrage gesendet.	Dieser Status kann auftreten, wenn der verwaltete Server nicht ordnungsgemäß heruntergefahren wurde. Stellen Sie sicher, dass der Administrator des verwalteten Servers über diese Situation informiert ist. Nehmen Sie, wenn nötig, Kontakt mit dem Administrator auf.
Deaktiviert	Dieser Status wird manuell über die Konsole festgelegt. Wenn sich ein Agent im Status Deaktiviert befindet, fragt der Agent alle 10 Minuten Befehle vom Server ab.	Senden Sie einen Befehl, um den Agent zu aktivieren (siehe *Agent-Befehle absenden auf Seite 6-4*).
Offline	Der Agent wurde nach dem Senden einer Abmeldeanfrage an den Remote Manager Server normal geschlossen. Ein Agent befindet sich in der Regel in diesem Status, wenn ein Benutzer den Agent-Dienst heruntergefahren hat oder der verwaltete Server heruntergefahren wurde.	Stellen Sie sicher, dass der Administrator des verwalteten Servers über diese Situation informiert ist. Nehmen Sie, wenn nötig, Kontakt mit dem Administrator des verwalteten Servers auf.
Unbekannt	Der Agent wird nicht ordnungsgemäß ausgeführt.	Entfernen Sie den Agent, und weisen Sie den Administrator des verwalteten Servers an, den Agent neu zu installieren. Wenden Sie sich an Ihren Supportanbieter, falls das Problem weiterhin besteht.
Plug-in-Fehler	Die Konsole hat Fehler in der Plug-in-Komponente des Agent-Dienstes entdeckt.	Entfernen Sie den Agent, und weisen Sie den Administrator des verwalteten Servers an, den Agent neu zu installieren. Wenden Sie sich an Ihren Supportanbieter, falls das Problem weiterhin besteht.

STATUS	BESCHREIBUNG	LÖSUNG
Nicht registriert	Der Agent ist nicht beim Remote Manager Server registriert.	Möglicherweise wurde der Agent nicht installiert oder kann nicht erfolgreich mit dem Remote Manager Server kommunizieren. Wenden Sie sich an den Administrator des verwalteten Servers.
Versionskonflikt	Die Versionen einiger der folgenden Komponenten sind nicht kompatibel: • Agent • Remote Manager • Worry-Free Business Security Standard und Worry-Free Business Security Advanced	Upgraden Sie den Agent und den verwalteten Server. Falls dies nicht möglich ist, melden Sie das Problem an den Administrator des Trend Micro Rechenzentrums.

Agent-Befehle absenden

Mit Agent-Befehlen können Sie Probleme in Zusammenhang mit dem Worry-Free Business Security (Standard und Advanced) Agent remote beheben. Wenn der Status eines Agent ungewöhnlich oder nicht registriert lautet, können Sie keinen Befehl an den Agent senden

Prozedur

1. Wechseln Sie zu **Kunden** > **{Kunden}** > **{Produkt}** > **Gruppen (Registerkarte)**.+

   Wählen Sie einen der folgenden Befehle:

   - **Jetzt durchsuchen**: Startet einen Suchvorgang für den Endpunkt.
   - **Suche beenden**: Beendet den Suchvorgang.

2. Wechseln Sie zu **Kunden** > **{Kunden}** > **{Produkt}** > **Domäneneinstellungen (Registerkarte)**.

Wählen Sie einen der folgenden Befehle:

- **Aktivieren**: Setzt den Agent aus dem deaktivierten Status in den normalen Funktionsstatus zurück.
- **Deaktivieren**: Agent beendet die Erfassung von Informationen, fragt aber weiterhin alle 10 Minuten Befehle vom Server ab.
- **Schwachstellenbewertung starten**: Führt eine Schwachstellenbewertungssuche aus.
- **Damage Cleanup Services starten**: Durchsucht Computer und beseitigt dateibasierte und Netzwerkviren sowie Überreste von Viren und Würmern auf Computern.

3. Wechseln Sie zu **Kunden** > **{Kunden}** > **{Produkt}** > **Verwalteter Server (Registerkarte)**.

   Wählen Sie einen der folgenden Befehle:

   - **Verwalteten Server aktualisieren**: Lädt Updates für verwaltete Server herunter und installiert sie.
   - **Security Agent aktualisieren**: Lädt Agent-Updates herunter und installiert sie.

Agent-Details anzeigen

Prozedur

1. Navigieren Sie zu **Kunden** > **{Kunde}** > **Produkte (Registerkarte)** > **WFBS-S/ WFBS-A** > **Endpunkt**.

   Die folgenden Informationen werden angezeigt:

   - **Status**
   - **Name**

- **GUID**: Globally Unique Identifier; Remote Manager erzeugt diese Zeichenfolge automatisch. Wird vom Administrator benötigt, der das Agent-Programm installiert.
- **IP-Adresse**: Die IP-Adresse des Servers, auf dem der Agent installiert wird.
- **Registriert am**
- **Letztes Update**: Datum und Uhrzeit des letzten Agent-Updates.
- **Agent-Version**
- **Verwaltetes Produkt**: Das durch den Agent verwaltete Produkt.
- **Version des verwalteten Produkts**: Version des durch den Agent verwalteten Produkts.

Agents über den verwalteten Server verwalten

Dieser Abschnitt enthält Informationen zum Verwalten von Agents über den verwalteten Server.

Agent-Statusmeldungen

Auf dem verwalteten Server zeigt der Agent eines der folgenden Task-Leistensymbole an:

TABELLE 6-2. Symbole der Task-Leiste

SYMBOL	BESCHREIBUNG
	Ein grünes Symbol zeigt an, dass der Agent mit dem Kommunikationsserver von Remote Manager verbunden ist. Der Agent wird ordnungsgemäß ausgeführt.
	Ein rotes Symbol zeigt an, dass der Agent nicht mit dem Kommunikationsserver von Remote Manager verbunden ist oder die Version des Agents nicht mit der des Servers übereinstimmt und aktualisiert werden muss.

SYMBOL	BESCHREIBUNG
	Ein rotes Symbol mit einem roten Pfeil zeigt an, dass der Agent von Remote Manager abgemeldet ist.
	Ein Symbol mit einem roten "X" bedeutet, dass der Agent deaktiviert wurde.

Die Agent-GUID auf dem verwalteten Server ändern

Wenn bei der Installation des Remote Manager Agents eine falsche GUID (Globally Unique Identifier) eingegeben wurde, löschen Sie den Agent und installieren Sie ihn unter Verwendung der richtigen GUID erneut. Wenn Sie diesen Vorgang nicht ausführen können, können Sie Folgendes tun:

Prozedur

1. Wechseln Sie zu `C:\Programme\Trend Micro\TMRMAgentForCSM`.
2. Öffnen Sie die Datei `AgentSysConfig.xml` in einem Texteditor.
3. Suchen Sie die GUID zwischen den Parametern `<AgentGUID>` und `</AgentGUID>`.
4. Bearbeiten Sie die GUID, und speichern Sie die Datei.
5. Öffnen Sie die Datei `csmSysConfig.xml` im selben Ordner mit einem Texteditor.
6. Suchen Sie die GUID zwischen den Parametern `<ProductGUID>` und `</ProductGUID>`.
7. Bearbeiten Sie die GUID, und speichern Sie die Datei.
8. Klicken Sie mit der rechten Maustaste auf das Symbol des Trend Micro Remote Manager Agents in der Task-Leiste, und klicken Sie auf **Dienst neu starten**.

Agent-Konfigurationstool verwenden

Mit Hilfe des Agent-Konfigurationstools können Sie Änderungen an den Konfigurationseinstellungen des Remote Manager Agents vornehmen.

Navigieren Sie zu **Start** > **Programme** > **Trend Micro Remote Manager Agent** > **Agent Configuration Tool** oder klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol und klicken Sie dann auf **Konfigurieren**.

Weitere Informationen finden Sie unter *Agent-Konfiguration auf Seite 6-8*.

Agent-Konfiguration

Agent-Konfigurationsmenü

Um den Agent zu konfigurieren, klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol und öffnen Sie das folgende Menü:

ABBILDUNG 6-1. Kontextmenü des Agent-Konfigurationstools

Die folgenden Elemente werden angezeigt:

- **Konfigurieren**: Öffnet das Agent-Konfigurationsfenster.
- **Sprache auswählen**: Zusätzlich zu anderen möglichen Sprachen ist "Englisch" immer verfügbar.
- **Dienst**: Starten, Beenden, Neu starten.

- **Beenden**: Durch das Beenden des Tools wird der Remote Manager Service nicht beendet. Es wird nur das Konfigurationstool geschlossen und das Symbol aus der Task-Leiste entfernt. Das Tool kann jederzeit erneut gestartet werden.

Hauptdialog des Konfigurationstools

Klicken Sie mit der rechten Maustaste auf das Task-Leistensymbol, und klicken Sie auf **Konfigurieren** im Agent-Konfigurationsmenü, um die Registerkarte **Allgemein** des Agent-Konfigurationstools zu öffnen.

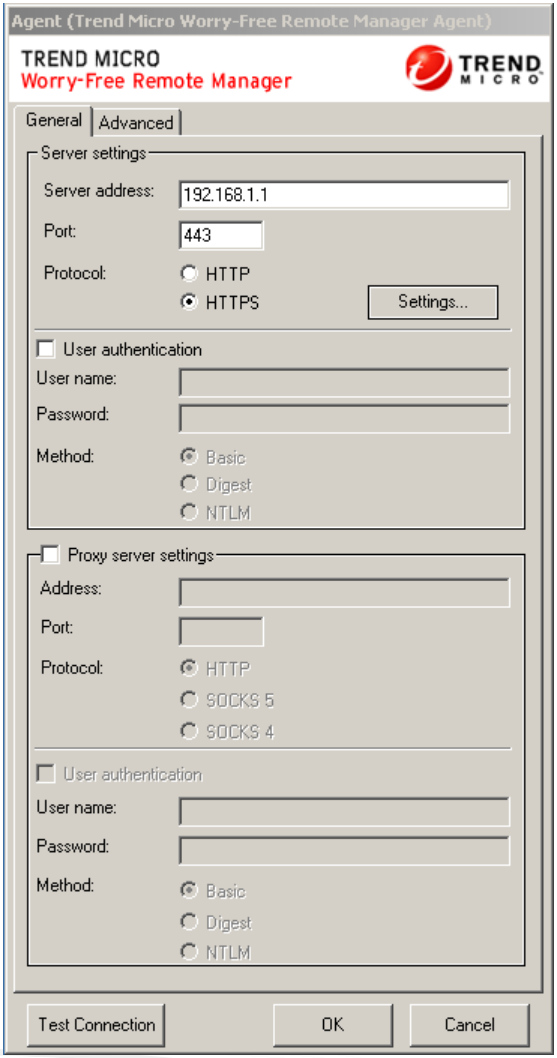


ABBILDUNG 6-2. Registerkarte "Allgemein" des Agent-Konfigurationstools

Die folgenden Bereiche des Agent-Konfigurationsfensters sind die einzigen zurzeit relevanten Bereiche dieses Tools.

- **Servereinstellungen**: Konfigurieren Sie die Serverkommunikation mit den folgenden Einstellungen:
  - **Serveradresse**: Vollqualifizierter Domänenname (FQDN) des Remote Manager Kommunikationsservers. Der FQDN ist je nach Region unterschiedlich:
    - **Asiatisch-pazifischer Raum**: `rm-apaca.trendmicro.com`
    - **Europa und Naher Osten**: `rm-emea.trendmicro.com`
    - **Japan**: `rm-jpa.trendmicro.com`
    - **Lateinamerika**: `rm-lara.trendmicro.com`
    - **Nordamerika**: `rm-usa.trendmicro.com`
  - **Port**: Der Port, über den der Remote Manager Server mit dem Agent kommuniziert. Dieser sollte 80 für HTTP und 443 für HTTPS sein.
  - **Protokoll**: Das Protokoll, das für die Kommunikation zwischen Server und Agent verwendet wird.
- **Proxy-Server-Einstellungen**: Aktivieren Sie diesen Bereich durch Klicken auf das Kontrollkästchen **Proxy-Server-Einstellungen**, falls das Netzwerk des Benutzers zur Kommunikation mit dem Remote Manager Server einen Proxy benötigt.
  - **Adresse**: Die IP-Adresse des Proxy-Servers.
  - **Port**: Der Port des Proxy-Servers.
  - **Protokoll**
- **Schaltfläche Verbindung testen**: Die Schaltfläche **Verbindung testen** wird zum Testen der Verbindung zwischen Agent und Remote Manager Server verwendet. Verwenden Sie diese Funktion, um die Verbindung zum Kommunikationsserver allgemein zu testen. Falls der Test fehlschlägt (wenn das Tool keine Verbindung mit dem Server herstellen kann, erscheint ein Popup-Dialogfeld), liegen möglicherweise allgemeine Probleme beispielsweise bei Adresse und Port des Kommunikationsservers oder des Proxy-Servers vor.

Agent-Einstellungen sichern und wiederherstellen

Falls Sie innerhalb von drei Tagen den Agent mit derselben GUID deinstallieren und dann erneut installieren müssen, behalten Sie die Agent-Einstellungen bei, um Datenüberlappungen zu vermeiden. Sichern Sie zu diesem Zweck die Konfigurationsdateien manuell, und ersetzen Sie dann nach der Neuinstallation des Agents die Konfigurationsdateien durch die Sicherungskopien.

Einstellungen sichern

Prozedur

1. Klicken Sie auf dem verwalteten Server mit der rechten Maustaste auf das Agent-Symbol in der Task-Leiste, und klicken Sie auf **Dienst beenden**, um den Agent-Dienst zu stoppen.

2. Kopieren Sie alle Dateien des Typs `.xml`, `.dat` und `.ini` aus dem Installationsordner `C:\Programme\ Trend Micro\WFRMAgentforCSM`.

   - `XML`-Dateien
     - `csmSysConfig.xml`
     - `csmLocalConfig.xml`
     - `csmLogDef.xml`
     - `AgentWorkConfig.xml`
     - `AgentSysConfig.xml`
     - `AgentStatus.xml`
     - `AgentLocalConfig.xml`
   - `DAT`-Dateien
     - `MSA.dat`

- `logBuf.dat`
- `group.dat`
- `CSA.dat`
- `CriticalVA.dat`

- `INI`-Dateien
  - `csmStatusData.ini`

3. Kopieren Sie alle Dateien aus dem Ordner `\Cache`.
4. Starten Sie den Agent-Dienst neu.

Einstellungen wiederherstellen

Prozedur

1. Deinstallieren Sie den Agent lokal, falls Sie das noch nicht getan haben. Ausführliche Hinweise finden Sie unter *Agents lokal entfernen auf Seite 6-16*.

Hinweis

Bei der lokalen Deinstallation des Agents meldet sich der Agent vom Remote Manager ab. Damit werden automatisch alle Daten in Zusammenhang mit dem Agent gelöscht. Wenn Sie verhindern möchten, dass sich der Agent abmeldet, ändern Sie vor der Deinstallation des Agents den Wert der Serveradresse in der Agent-Benutzeroberfläche.

2. Installieren Sie den Agent neu. Stellen Sie sicher, dass Sie dieselbe GUID wie in der Datei `agentSysConfig.xml` verwenden.
3. Klicken Sie auf dem verwalteten Server mit der rechten Maustaste auf das Agent-Symbol in der Task-Leiste, und klicken Sie auf **Dienst beenden**, um den Agent-Dienst zu stoppen.
4. Ersetzen Sie die Konfigurationsdateien durch die Sicherungsdateien.

5. Klicken Sie mit der rechten Maustaste auf das Agent-Symbol in der Task-Leiste, und klicken Sie auf **Dienst starten**, um den Agent-Dienst neu zu starten.

Build-Nummer des Agents suchen

Die können die Build-Nummer des Agents entweder in der Konsole oder direkt in dem Agent prüfen.

Über die Remote Manager Web-Konsole

Prozedur

1. Klicken Sie auf die Registerkarte **Kunden**.
2. Wählen Sie die Zieldomäne aus dem Listenfeld **Anzeigen nach** im linken Fensterbereich.
3. Klicken Sie auf **Alle Kunden** > **{Kunde}** > **{Agent}** > **Server-/Agent-Details** > **Details zum TMRM Agent**.
4. Prüfen Sie die Version des Agents in der Tabelle **Allgemeine Informationen**.

Im Agent

Prozedur

1. Wechseln Sie zum Verzeichnis `C:\Program Files\Trend Micro \WFRMAgentForCSM`.
2. Klicken Sie mit der rechten Maustaste auf die Datei `csmplugin.dll` und anschließend auf **Eigenschaften** > **Version (Registerkarte)**, um die Build-Nummer anzuzeigen.

Speicherorte der Agent-Protokolle und -Konfigurationsdateien

Die Agent-Konfigurationsdateien befinden sich unter:

- `<Installationspfad>\Trend Micro\WFRMAgentForCSM\*.xml`
- `<Installationspfad>\Trend Micro\WFRMAgentForCSM\*.ini`

Die Protokolldateien befinden sich unter:

- `<Installationspfad>\Trend Micro\WFRMAgentForCSM\log\`

Das Agent-Fehlerprotokoll aktivieren

In der Regel protokolliert der Agent nur Warnmeldungen und Fehlerinformationen. Wenn Sie weitere Protokollinformationen benötigen, aktivieren Sie das Agent-Fehlerprotokoll.

Lösung

1. Öffnen Sie die Datei `AgentLocalConfig.xml` unter `<install path>\Trend Micro\WFRMAgentForCSM\` in einem Texteditor.
2. Ändern Sie `<DebugLogLevel>` von `LL_FOR_ERROR` zu `LL_FOR_ALL`.
3. Starten Sie den Agent-Dienst neu, indem Sie mit der rechten Maustaste auf den Remote Manager Agent in der Task-Leiste klicken, und klicken Sie anschließend auf **Dienst neu starten**.
4. Die Agent-Protokolldatei befindet sich unter `<install path>\Trend Micro\WFRMAgentForCSM\log\TMICAgent.log`.

Agents entfernen

Dieser Abschnitt enthält Informationen zum Entfernen von Agents.

Agents lokal entfernen

Bevor Sie einen Agent entfernen, siehe *Agent-Einstellungen sichern und wiederherstellen auf Seite 6-12*.

Warnung!

Durch das Abmelden eines Agents aus Remote Manager werden alle mit dem Remote Manager Agent verknüpften Daten gelöscht. Um zu verhindern, dass sich der Agent abmeldet (und seine Daten löscht), ändern Sie vor der Deinstallation des Remote Manager Agents den Wert der Serveradresse in der Remote Manager Agent-Benutzeroberfläche.

Es gibt drei Möglichkeiten, um einen Remote Manager Agent lokal zu löschen:

- Remote Manager Agent direkt deinstallieren.
- Remote Manager Agent über die Systemsteuerung deinstallieren.
- Remote Manager Agent manuell deinstallieren.

Remote Manager Agent direkt deinstallieren

Prozedur

1. Öffnen Sie die Installationsdatei des Remote Manager Agents (`WFRMAgentforCSM.exe` oder `WFRMAgentforWFBS.exe`).
2. Klicken Sie auf **Ja**, um den Dialog **Deinstallation bestätigen** zu bestätigen.

   Hinweis

   Während der Deinstallation werden Sie zum Schließen bestimmter Anwendungen aufgefordert. Schließen Sie diese Anwendungen, und klicken Sie dann auf **Wiederholen**, um den Vorgang fortzusetzen.

3. Klicken Sie nach abgeschlossener Deinstallation auf **Fertig stellen**, um den Assistenten zu beenden.

Remote Manager Agent über die Systemsteuerung deinstallieren

Prozedur

1. Öffnen Sie das Applet **Software** in der Systemsteuerung (oder **Programme und Einstellungen** unter Windows Vista™).
2. Wählen Sie `Trend Micro Remote Manager Agent` und klicken Sie dann auf die Schaltfläche **Ändern/Entfernen**.
3. Folgen Sie den Anweisungen.

Remote Manager Agent manuell deinstallieren

Falls der Agent aus irgendeinem Grund mit keiner der Standardmethoden deinstalliert werden kann, versuchen Sie es mit folgenden Schritten:

Prozedur

1. Beenden Sie den Remote Manager Agent-Dienst.
   a. Gehen Sie zu **Start** > **Ausführen**.
   b. Geben Sie in der Befehlszeile `cmd` ein und drücken Sie die **Eingabetaste**.
   c. Führen Sie den folgenden Befehl aus:

      ```
      net stop Trend Micro Worry-Free Remote Manager Agent
      ```

2. Entfernen Sie den Remote Manager Agent-Dienst:
   a. Verwenden Sie in der Befehlszeile den Befehl zum Verzeichniswechsel (cd), um zum Verzeichnis des Remote Manager Agents zu wechseln.
   b. Führen Sie den folgenden Befehl aus:

      ```
      TMICAgent -u
      ```

3. Entfernen Sie die Programmdateien.

```
Delete {Agent install directory} / WFRMAgentForCSM
```

4. Öffnen Sie den Registrierungseditor (`regedit.exe`), und entfernen Sie die folgenden Registrierungsschlüssel:

Hinweis

Erstellen Sie immer eine Sicherungskopie, bevor Sie die Registrierung ändern. Fehlerhafte Registrierungsänderungen können schwerwiegende Probleme verursachen. In diesem Fall finden Sie im Hilfethema "Die Registrierung wiederherstellen" in `regedit.exe` oder "Einen Registrierungsschlüssel wiederherstellen" in `regedt32.exe` Informationen über die Wiederherstellung der Registrierung.

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMIC4CSM\Agent`
  `\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products`
  `\23FC8F347B51DD440AD13A73D13A73D22D58E6`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows`
  `\CurrentVersion\Installer\UserData\S-1-5-18\Products`
  `\23FC8F347B51DD440AD13A73D13A73D22D58E6`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows`
  `\CurrentVersion\Uninstall\{43F8CF32-15B7-44DD-A01D-`
  `A3372DD2856E}`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows`
  `\CurrentVersion\Uninstall\InstallShield Uninstall`
  `Information\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows`
  `\CurrentVersion\Uninstall\InstallShield_`
  `\{43F8CF32-15B7-44DD-A01D-A3372DD2856E}`

5. Entfernen Sie die Verknüpfung des Remote Manager Agents aus dem Windows Start-Menü.

   a. Klicken Sie auf dem Desktop auf **Arbeitsplatz**.

   b. Ändern Sie das aktuelle Verzeichnis in `..\Dokumente und Einstellungen\Alle Benutzer\Startmenü\Programme`.

c. Löschen Sie den Ordner Remote Manager Agent.

Kapitel 7

Lizenzen verwalten

Dieser Abschnitt enthält die folgenden Themen:

Hinweis

Diese Funktion kann nur angewendet werden, wenn Sie ein Konto verwenden, das in die Trend Micro Licensing Management Platform integriert ist.

- *Arbeitsplatzzuordnungen hinzufügen auf Seite 7-2*
- *Lizenzen verlängern auf Seite 7-3*

Arbeitsplatzzuordnungen hinzufügen

Jeder Reseller kann angeben, wie viele Arbeitsplätze pro Kunde zugeordnet werden können. Wenn die Anzahl der zugeordneten Arbeitsplätze überschritten wird, können Reseller weitere Arbeitsplätze pro Kunde zuordnen.

Hinweis

Diese Funktion kann nur angewendet werden, wenn Sie ein Konto verwenden, das in die Trend Micro Licensing Management Platform integriert ist.

Prozedur

1. Es gibt mehrere Möglichkeiten, das Fenster **Arbeitsplätze hinzufügen** anzuzeigen:
   - Über die Trend Micro™ Remote Manager™ Web-Konsole:
     a. Klicken Sie auf **Kunden**.
     b. Wählen Sie den Kunden aus, der die Anzahl an zugeordneten Arbeitsplätzen überschritten hat.
     c. Klicken Sie auf **Arbeitsplätze ändern**.
   - Klicken Sie im Widget **Benachrichtigungen** auf den Link **Jetzt Arbeitsplätze hinzufügen** neben der Benachrichtigung.
   - Klicken Sie in der E-Mail-Benachrichtigung auf die Schaltfläche **Jetzt Arbeitsplätze hinzufügen**.
2. Geben Sie die Anzahl der Arbeitsplätze ein, die Sie der Zuordnung hinzufügen möchten.
3. Klicken Sie auf **Absenden**.

Lizenzen verlängern

Verlängern Sie die Lizenzen für Kunden, die Sie verwalten.

Hinweis

Diese Funktion kann nur angewendet werden, wenn Sie ein Konto verwenden, das in die Trend Micro Licensing Management Platform integriert ist.

Prozedur

1. Es gibt mehrere Möglichkeiten, das Fenster **Lizenzen verlängern** anzuzeigen:
   - Über die Remote Manager Web-Konsole:
     a. Klicken Sie auf **Kunden**.
     b. Wählen Sie den Kunden aus, dessen Lizenz abgelaufen ist oder demnächst abläuft.
     c. Klicken Sie auf **Lizenz verlängern**.
   - Klicken Sie im Widget **Benachrichtigungen** auf den Link **Jetzt verlängern** neben der Benachrichtigung.
   - Klicken Sie in der E-Mail-Benachrichtigung auf die Schaltfläche **Jetzt verlängern**.
2. Geben Sie die Änderungen in den Lizenzbedingungen an.
3. Klicken Sie auf **Absenden**.

Kapitel 8

Einstellungen verwalten

Dieser Abschnitt enthält die folgenden Themen:

- *Benachrichtigungen konfigurieren auf Seite 8-2*
- *Konsoleneinstellungen konfigurieren auf Seite 8-3*
- *Standardeinstellungsvorlagen konfigurieren auf Seite 8-4*

Benachrichtigungen konfigurieren

Richten Sie Benachrichtigungen ein, falls ein Ereignis auftritt, das Ihre Aufmerksamkeit erfordert. Diese Benachrichtigungen können entweder per E-Mail, über das Widget **Benachrichtigungen** oder über eine Drittanbietersoftware erfolgen.

Prozedur

1. Konfigurieren Sie die allgemeinen Einstellungen für Benachrichtigungen.

   a. Klicken Sie auf **Administration** > **Benachrichtigungen konfigurieren**.

   Hinweis

   In diesem Fenster wird die E-Mail-Adresse angezeigt, an die die E-Mail-Benachrichtigung gesendet wird. Wenn diese falsch ist, wechseln Sie zu **Mein Konto** oder zur Licensing Management Platform Web-Konsole und ändern Sie die Einstellungen für das Profil.

   b. Wählen Sie die Sprache aus.

   c. (Optional) Aktivieren oder deaktivieren Sie die tägliche E-Mail mit einem Benachrichtigungsüberblick. Wenn Sie diese Einstellung aktivieren, erhalten Sie täglich eine E-Mail, mit der Sie über alle Ereignisse informiert werden, die ausgelöst wurden und für die entsprechende Maßnahmen erforderlich sind.

   d. Geben Sie die Arten von Benachrichtigungen an, die gesendet werden, wenn Ereignisse ausgelöst werden:

      - **In Benachrichtigungen anzeigen**: Sie können Benachrichtigungen zu diesem Ereignis im Widget "Benachrichtigungen" sehen. Sie können die Anzahl an Ereignissen auch über das Symbol "Benachrichtigungen" im Bannerbereich der Konsole anzeigen.
      - **E-Mail:** Sie erhalten eine Benachrichtigung per E-Mail zu diesem Ereignis. Mit den in dieser E-Mail bereitgestellten Links haben Sie beispielsweise die Möglichkeit, Lizenzen zu verlängern oder direkt zugeordnete Arbeitsplätze hinzuzufügen.

   e. Klicken Sie auf **Speichern**.

2. Konfigurieren Sie die kundenspezifischen Einstellungen für Benachrichtigungen.

   a. Navigieren Sie zu **Kunde** > **{Kundenname}** > **Benachrichtigungen (Registerkarte)**.

   b. Wählen Sie die Einstellung für Benachrichtigungen aus.

   c. Geben Sie zusätzliche Empfänger an.

> **Hinweis**
>
> Stellen Sie sicher, dass die Kunden über integrierte Tools von Drittanbietern verfügen, bevor Sie Benachrichtigungen für Kaseya, Autotask oder ConnectWise aktivieren.

Konsoleneinstellungen konfigurieren

Geben Sie das Logo an, das den Kunden angezeigt wird, wenn sie sich beim Service anmelden.

> **Hinweis**
>
> Es handelt sich um eine optionale Einstellung.

Prozedur

1. Klicken Sie auf **Administration** > **Konsoleneinstellungen**.
2. Wählen Sie das Bild aus, das Sie verwenden möchten. Das Logo muss ein `PNG`-, `JPG`-, `BMP`- oder `GIF`-Bild mit den maximalen Abmessungen von 600 x 55 Pixel (Breite x Höhe) sein.
3. Klicken Sie auf **Speichern**.

Standardeinstellungsvorlagen konfigurieren

Hinweis

Standardeinstellungsvorlagen sind nur verfügbar, wenn Sie Trend Micro Remote Manager in die Licensing Management Platform integriert haben, und sie gelten nur für Ihr Worry-Free Business Security Services-Produkt.

Bei den Standardeinstellungsvorlagen handelt es sich um Vorlagen, die bereits vorkonfigurierte Einstellungen für einen Kunden enthalten. Dadurch kann einfacher sichergestellt werden, dass die Kunden dieselben Einstellungen verwenden.

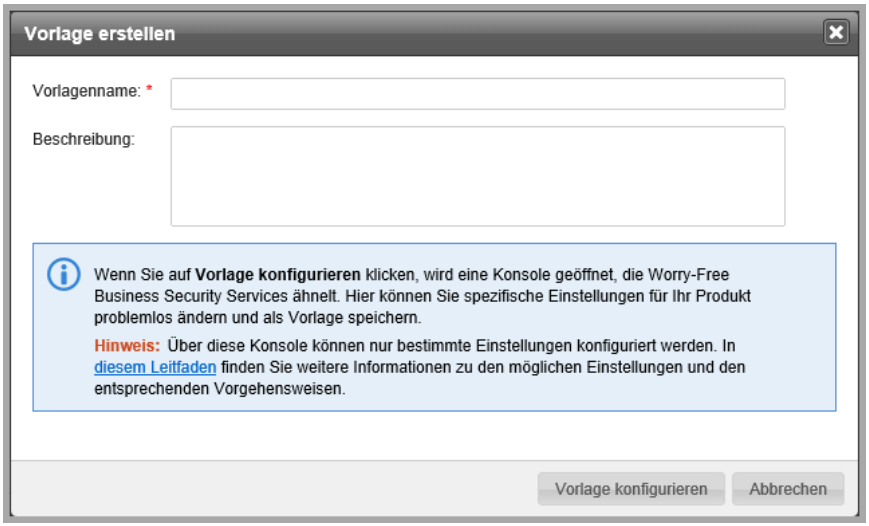
Beim Erstellen der Vorlagen wird eine Konsole angezeigt, die Worry-Free Business Security Services ähnelt. Dies soll Ihnen Vertrautheit bieten, wenn Sie die Standardeinstellungen einrichten, die die einzelnen Kunden verwenden sollen. Sie können verschiedene Vorlagen erstellen, die spezifisch für Kundentypen oder -gruppen sind.

Weitere Informationen zu den Einstellungen, die Sie über diese Vorlage konfigurieren können, finden Sie in der Worry-Free Business Security Services-Dokumentation unter:

http://docs.trendmicro.com/de-de/smb/worry-free-business-security-services.aspx

Prozedur

1. Navigieren Sie zu **Administration** > **Standardeinstellungsvorlagen konfigurieren**.
2. Klicken Sie auf **Erstellen**.


Vorlage erstellen
Vorlagenname: *
Beschreibung:
Wenn Sie auf Vorlage konfigurieren klicken, wird eine Konsole geöffnet, die Worry-Free Business Security Services ähnelt. Hier können Sie spezifische Einstellungen für Ihr Produkt problemlos ändern und als Vorlage speichern.
Hinweis: Über diese Konsole können nur bestimmte Einstellungen konfiguriert werden. In diesem Leitfaden finden Sie weitere Informationen zu den möglichen Einstellungen und den entsprechenden Vorgehensweisen.
Vorlage konfigurieren
Abbrechen

3. Geben Sie den Namen der Vorlage sowie einige Kommentare oder Beschreibungen ein. Dies erleichtert Ihnen die Erinnerung, wofür oder für wen diese Vorlage verwendet werden kann.

4. Klicken Sie auf **Vorlage konfigurieren**.

Hinweis

Eine Konsole, die Worry-Free Business Security Services ähnelt, wird geöffnet. Alle Änderungen, die Sie an dieser Website vornehmen, werden als Vorlage gespeichert und haben keine Auswirkungen auf registrierte Produkte.

5. Konfigurieren Sie die folgenden Einstellungen:

   - Richtlinien

     a. Navigieren Sie zu **Geräte** > **Server (Standard)** > **Richtlinien konfigurieren**.

     b. Konfigurieren Sie die Richtlinieneinstellungen für den Standardserver.

     c. Navigieren Sie zu **Suche** > **Gerät (Standard)** > **Richtlinien konfigurieren**.

d. Konfigurieren Sie die Richtlinieneinstellungen für das Standardgerät.

e. Klicken Sie auf **Speichern**.

- Sucheinstellungen

  a. Navigieren Sie zu **Suche** > **Manuelle Suche (Registerkarte)**.

  b. Konfigurieren Sie die Standardeinstellungen für Server und Geräte.

  c. Navigieren Sie zu **Suche** > **Zeitgesteuerte Suche (Registerkarte)**.

  d. Konfigurieren Sie die Standardeinstellungen für Server und Geräte.

  e. Klicken Sie auf **Speichern**.

- Einstellungen für die Benachrichtigung

  a. Navigieren Sie zu **Administration** > **Benachrichtigungen** > **Ereignisse (Registerkarte)**.

  b. Geben Sie die Ereignisse und Empfänger an, bei denen eine Ereignisbenachrichtigung ausgelöst wird.

  c. Klicken Sie auf **Speichern**.

- Allgemeine Einstellungen

  a. Navigieren Sie zu **Administration** > **Allgemeine Einstellungen** > **Sicherheitseinstellungen (Registerkarte)**.

  b. Nehmen Sie die erforderlichen Änderungen bei den Einstellungen für die Suche, Verhaltensüberwachung oder Ausbruchsprävention vor.

  c. Navigieren Sie zu **Administration** > **Allgemeine Einstellungen** > **Zulässige/Gesperrte Einstellungen (Registerkarte)**.

  d. Fügen Sie Websites zur Liste der zulässigen oder gesperrten Websites hinzu oder entfernen Sie Websites aus dieser Liste.

  e. Navigieren Sie zu **Administration** > **Allgemeine Einstellungen** > **Agent-Steuerung (Registerkarte)**.

  f. Ändern Sie die Agent-Einstellungen.

g. Navigieren Sie zu **Administration** > **Allgemeine Einstellungen** > **Geräteverwaltung (Registerkarte)**.

h. Ändern Sie die benutzerbasierten Einstellungen für die Geräteverwaltung.

i. Klicken Sie auf **Speichern**.

Kapitel 9

Ereignisse verwalten

Dieser Abschnitt enthält die folgenden Themen:

- *Ereignisse verwalten auf Seite 9-2*
- *Ereignisse anzeigen auf Seite 9-4*
- *Ereignistypen auf Seite 9-5*

Ereignisse verwalten

In Trend Micro Remote Manager findet ein Ereignis statt, wenn ein Produkt oder Service an einem Kundenstandort Ihre Aufmerksamkeit erfordert. Verwenden Sie das Fenster **Vorfallprotokolle**, um die Ereignisse aller Ihrer Kunden zu überprüfen und zu verwalten. Sie können nach Ereignissen, die in Worry-Free Business Security, Worry-Free Business Security Services, Hosted Email Security, Cloud Edge und InterScan Web Security as a Service aufgetreten sind, nach Typ oder nach Kunden suchen. Sie können die Ereignisse nach Schweregrad und Status filtern.

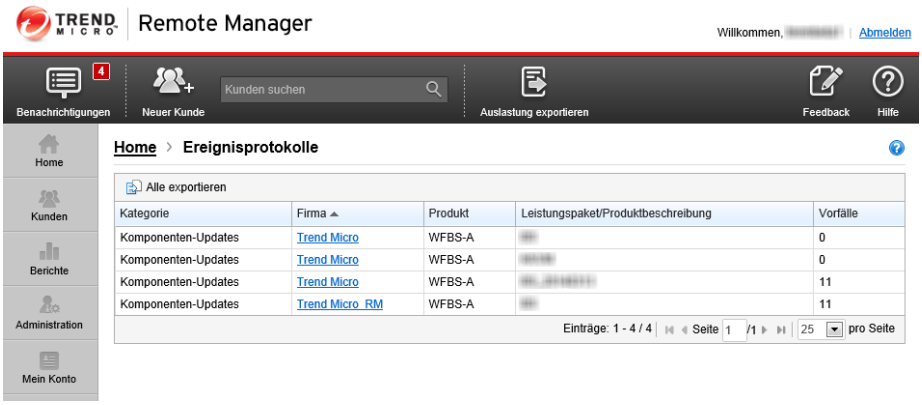


ABBILDUNG 9-1. Fenster Vorfallprotokolle mit Antiviren-Ereignissen

Ereignisse

Ereignisse werden wie folgt kategorisiert:

- Bedrohungen
  - *Ausbruchsschutz auf Seite 9-5*
  - *Antivirus auf Seite 9-7*
  - *Anti-Spyware auf Seite 9-9*
  - *Anti-Spam auf Seite 9-11*

- *Netzwerkvirus auf Seite 9-11*
- *Web Reputation auf Seite 9-12*
- *Verhaltensüberwachung auf Seite 9-13*
- *URL-Filter auf Seite 9-13*
- *Gerätesteuerung auf Seite 9-14*

- System
  - *Smart Protection Service auf Seite 9-14*
  - *Komponenten-Update auf Seite 9-15*
  - *Speichernutzung auf Seite 9-16*
- Lizenz
  - Lizenz abgelaufen
  - Lizenz läuft in Kürze ab
  - Lizenznutzung

Infektionsgrad

Schweregrad wird wie folgt kategorisiert:

- **Aktion erforderlich**: Ereignisse, die sofortige Aufmerksamkeit erfordern.
- **Achtung**: Warnungen oder Benachrichtigungen sind nur zu Ihrer Information bestimmt.

Status

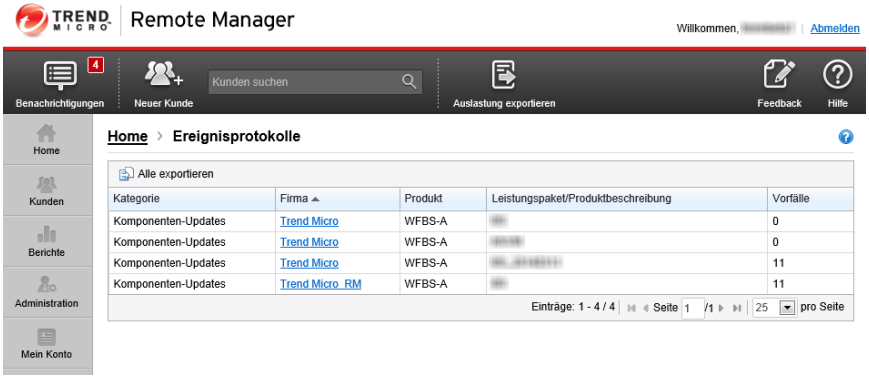
Status wird wie folgt kategorisiert:

- **Ungelöst**: Diese Ereignisse erfordern Ihre Aufmerksamkeit.
- **Wird zurückgesetzt/aktualisiert**: Sie haben diese Ereignisse bearbeitet und sie warten auf eine Aktualisierung vom Produkt/Service.

Ereignisse anzeigen

Prozedur

1. Gehen Sie zu **Home** > **{Dashboard}** > **{Widget}**
2. Klicken Sie auf einen der Vorfälle.



3. Führen Sie eine der folgenden Schritte durch:
   - Vorfälle nach Typ oder Kunden mit Hilfe der Struktur und des Suchfensters auf der linken Seite anzeigen
   - Ereignisse für bestimmte Produkte/Services mit Hilfe der Registerkarten auf der rechten Seite anzeigen
   - Ereignisse nach Schweregrad oder Status mit Hilfe der Listenfelder oben rechts im Fenster anzeigen
   - Zu einem bestimmten Ereignis wechseln, indem Sie auf Links in Widgets oder Benachrichtigungen klicken, um weitere Informationen anzuzeigen
   - Ein Ereignis auswählen und auf **Zurücksetzen** klicken, um Zähler zurückzusetzen oder auf **Aktualisieren** klicken, um Komponenten zu aktualisieren.

Informationen zu den einzelnen Ereignissen und zu ergreifenden Maßnahmen finden Sie unter *Ereignistypen auf Seite 9-5*.

Ereignistypen

Hier werden die verschiedenen Ereignistypen angezeigt, die Ihnen über Trend Micro Remote Manager angezeigt werden.

Details des Ausbruchsschutzstatus

Hinweis

Dies ist nur für Worry-Free Business Security (alle) verfügbar.

Der Ausbruchsschutz warnt frühzeitig vor Internet-Bedrohungen und anderen weltweiten Ausbruchsbedingungen. Der Ausbruchsschutz reagiert automatisch mit Vorkehrungsmaßnahmen zum Schutz von Computern und Netzwerk. Im Anschluss daran folgen Schutzmaßnahmen zur Problemfeststellung und Schadensbehebung. Der Ausbruchsschutz schützt Netzwerke und Clients. Währenddessen arbeiten *TrendLabs auf Seite 12-5* an einer Lösung zur Bekämpfung dieser Bedrohung. Sobald TrendLabs eine Lösung gefunden hat, werden aktualisierte Komponenten veröffentlicht, die von Worry-Free Business Security (alle) Servern heruntergeladen und auf Clients verteilt werden. Der Ausbruchsschutz entfernt daraufhin sämtliche Virenüberreste und behebt den durch die Bedrohung entstandenen Schaden an Dateien und Verzeichnissen.

Der Ausbruchsschutz kann im Falle eines Ausbruchs die folgenden Aktionen durchführen:

- Ports sperren
- Bestimmte Dateien und Verzeichnisse mit Schreibschutz versehen
- Bestimmte Anhänge sperren

Um den Ausbruchsschutzstatus für verwaltete Netzwerke zu ermitteln, überprüft Trend Micro, ob TrendLabs einen Virenalarm ausgelöst hat. Ein Ausbruchsschutzereignis wird

auf dem Dashboard nur dann angezeigt, wenn ein oder mehrere Ausbruchsschutzereignisse aufgetreten sind.

Die unten stehende Tabelle zeigt mögliche Ausbruchsschutz-Statussymbole an.

TABELLE 9-1. Symbole für den Ausbruchsschutzstatus

STATUSSYMBOL	BESCHREIBUNG
	TrendLabs hat Alarmstufe Gelb ausgelöst
	TrendLabs hat Alarmstufe Rot ausgelöst

Alarmstatus

Informationen über den Alarmstatus werden bei Alarmstufe Rot oder Gelb angezeigt. Aktivieren Sie den Ausbruchsschutz, damit vorbeugende Maßnahmen automatisch durchgeführt werden und das Netzwerk geschützt ist, solange noch kein Pattern-Update verfügbar ist.

Anfällige Computer

Anfällige Computer sind Computer, die noch keine Patches für bekannte Software-Sicherheitslücken haben. Informieren Sie den Administrator der betroffenen Domäne über die Namen der anfälligen Computer und die Sicherheitslücken. Um diese Informationen zu erhalten, klicken Sie auf die Zahl der anfälligen Computer.

Führen Sie eine Suche zur Schwachstellenbewertung durch, um sicherzustellen, dass die Liste der betroffenen Computer auf dem aktuellen Stand ist. Weitere Informationen finden Sie unter *Worry-Free Business Security Befehle auf Seite 3-34*.

Zu säubernde Computer

Zu säubernde Computer sind Computer, auf denen sich Viren oder Malware befinden, die der Sicherheits-Client nicht entfernen, löschen oder in Quarantäne verschieben konnte. Auf einem infizierten Computer wird gewöhnlich eine Kopie des Virus oder der Malware ausgeführt, der/die den Computer so konfiguriert hat, dass ein automatisches Starten und weiteres Ausführen des Virus/der Malware ermöglicht wird.

Klicken Sie auf die Anzahl der zu säubernden Computer, um eine Liste der infizierten Computer und die Namen der Viren anzuzeigen. Verteilen Sie bei infizierten Computern Damage Cleanup Services (DCS) in der Domäne. Weitere Informationen finden Sie unter *Worry-Free Business Security Befehle auf Seite 3-34*.

Details des Antiviren-Status

Hinweis

Dies ist nur für Worry-Free Business Security (alle) verfügbar.

Die unten stehende Tabelle enthält mögliche Antiviren-Statussymbole und ihre Farbcodierung.

TABELLE 9-2. Symbole des Antiviren-Status

STATUSSYMBOL	BESCHREIBUNG
	Dieses Statussymbol wird angezeigt, wenn 15 oder mehr Spyware-/Grayware-Vorfälle innerhalb einer Stunde gefunden wurden (Worry-Free Business Security (alle), Standard). Administratoren können den Grenzwert auf dem verwalteten Server ändern. Das Einstundenintervall ist der 60-Minuten-Zeitraum vor dem Bewertungszeitpunkt.
	Dieses Statussymbol wird angezeigt, wenn eine der folgenden Bedingungen zutrifft: • Die Echtzeitsuche auf dem Exchange Server ist deaktiviert. • Ein Security-Client kann Malware nicht entfernen oder in Quarantäne verschieben. • Bei Worry-Free Business Security Standard oder Worry-Free Business Security Advanced 5.1 oder höher: Die Echtzeitsuche ist auf mindestens einem Computer deaktiviert.

Virenvorfälle

Virenvorfälle sind die Anzahl der Viren- oder Malware-Funde in der Domäne. In der Konsole sind diese statistischen Informationen in folgende Gruppen unterteilt:

- **Desktop/Server**: bei manuellen Suchen oder beim Zugriff auf Dateien auf Desktop- und Servercomputern entdeckte Viren oder Malware
- **Exchange Server**: Viren oder Malware in E-Mail-Nachrichten, die von einem Exchange Server verarbeitet werden

Greifen Sie auf weitere Informationen oder Aktionen – sofern verfügbar – zu, indem Sie auf **Details** klicken.

Warnung!

Klicken Sie nur dann auf **Zurücksetzen**, wenn Sie sicher sind, dass die Vorfälle bearbeitet wurden und unter Kontrolle sind.

Antivirenaktion fehlgeschlagen

Antiviren-Scanner säubern, löschen oder verschieben Dateien in Quarantäne, in denen Malware oder Viren gefunden wurden. Wenn die erste Aktion fehlschlägt, wird normalerweise die zweite Aktion durchgeführt.

Fehlgeschlagene Aktionen deuten darauf hin, dass ein Virus oder eine Malware die Antiviren-Mechanismen erfolgreich umgangen und den Computer infiziert hat. Remote Manager betrachtet Computer als infiziert, wenn Viren oder Malware nicht entfernt, in Quarantäne verschoben oder gelöscht werden konnten.

Greifen Sie auf weitere Informationen oder Aktionen – sofern verfügbar – zu, indem Sie auf **Details** klicken.

Zu säubernde Computer

Zu säubernde Computer sind Computer, auf denen sich Viren oder Malware befinden, die der Sicherheits-Client nicht entfernen, löschen oder in Quarantäne verschieben konnte. Auf einem infizierten Computer wird gewöhnlich eine Kopie des Virus oder der Malware ausgeführt, der/die den Computer so konfiguriert hat, dass ein automatisches Starten und weiteres Ausführen des Virus/der Malware ermöglicht wird.

Klicken Sie auf die Anzahl der zu säubernden Computer, um eine Liste der infizierten Computer und die Namen der Viren anzuzeigen. Verteilen Sie bei infizierten Computern

Damage Cleanup Services (DCS) in der Domäne. Weitere Informationen finden Sie unter *Worry-Free Business Security Befehle auf Seite 3-34*.

Verteilen Sie Damage Cleanup Services (DCS) auf die Domain, wenn Computer wegen fehlgeschlagener Antiviren-Aktionen infiziert wurden. Weitere Informationen finden Sie unter *Worry-Free Business Security Befehle auf Seite 3-34*.

Echtzeitsuche deaktiviert

Bei Computern mit deaktivierter Echtzeitsuche können Dateien nicht durchsucht werden, sobald diese eingehen oder bearbeitet werden. Diese Dateien werden jedoch bei Durchführung der zeitgesteuerten Suche durchsucht. Diese Computer sind in höchstem Maße anfällig für Viren- oder Malware-Infektionen. Exchange Server mit deaktivierter Echtzeitsuche lassen alle Dateien (auch diejenigen, die mit Malware infiziert sind) in E-Mail-Nachrichten durch und machen das Kundennetzwerk dadurch anfällig für Massenmail-Würmer.

Greifen Sie auf weitere Informationen oder Aktionen – sofern verfügbar – zu, indem Sie auf **Details** klicken.

Um die Echtzeitsuche auf allen Computern und Exchange Servern in der Domäne zu aktivieren, wählen Sie den Kunden aus und klicken Sie auf **Lösen**.

Details des Anti-Spyware-Status

Hinweis

Anti-Spyware ist nur für Worry-Free Business Security (alle) verfügbar.

Der Anti-Spyware-Status wird auf der Seite **Kunden** mit Statussymbolen und Farbcodierung angezeigt, die auf eine relativ hohe Zahl von Spyware-/Grayware-Vorfällen und das Vorhandensein mit Spyware/Grayware infizierter Computer hindeuten.

Die unten stehende Tabelle zeigt mögliche Anti-Spyware-Statussymbole an.

TABELLE 9-3. Anti-Spyware-Statussymbole

STATUSSYMBOL	BESCHREIBUNG
	15 oder mehr Spyware-/Grayware-Vorfälle wurden innerhalb einer Stunde gefunden (Worry-Free Business Security (alle), Standard). Sie können den Grenzwert auf dem verwalteten Server ändern. Das Einstundenintervall ist der 60-Minuten-Zeitraum vor dem Bewertungszeitpunkt.
	Aktion erforderlich. Mindestens ein Computer muss neu gestartet werden, um eine Spyware-/Grayware-Infektion vollständig zu entfernen.

Neustart des Computers zur Beseitigung von Anti-Spyware

"Neustart des Computers für Anti-Spyware erforderlich" zeigt die Anzahl der mit Spyware/Grayware infizierten Computer, die teilweise gesäubert wurden. Diese Computer bleiben infiziert, da die betreffende Spyware/Grayware nur durch einen Neustart vollständig entfernt werden kann. Weisen Sie einen Administrator beim Kunden an, die Computer manuell neu zu starten, um die Säuberung dieser Computer abzuschließen.

Greifen Sie auf weitere Informationen oder Aktionen – sofern verfügbar – zu, indem Sie auf **Details** klicken.

Warnung!

Klicken Sie nur dann auf **Zurücksetzen**, wenn Sie sicher sind, dass die Vorfälle bearbeitet wurden und unter Kontrolle sind.

Spyware-/Grayware-Vorfälle

Spyware-/Grayware-Vorfälle sind die Anzahl der Spyware-/Grayware-Funde in der Domäne. Um eine Liste der betroffenen Computer und die Namen der Spyware-/Grayware-Bedrohungen anzuzeigen, klicken Sie auf die Anzahl der Vorfälle. Klicken Sie auf **Zurücksetzen**, um den aktuellen Zähler zurückzusetzen.

Greifen Sie auf weitere Informationen oder Aktionen – sofern verfügbar – zu, indem Sie auf **Details** klicken.

Warnung!

Klicken Sie nur dann auf **Zurücksetzen**, wenn Sie sicher sind, dass die Vorfälle bearbeitet wurden und unter Kontrolle sind.

Details des Anti-Spam-Status

Der Abschnitt zu Anti-Spam enthält Warnungen zur wachsenden Anzahl von Spam-Nachrichten, die der Exchange Server verarbeitet. In dem Fenster zeigen Statussymbole, ob der Prozentsatz der Spam-Nachrichten (auf Basis aller von Exchange Servern verarbeiteten Nachrichten) einen bestimmten Grenzwert erreicht hat. Ein Anti-Spam-Ereignis wird auf dem Dashboard nur dann angezeigt, wenn ein oder mehrere Anti-Spam-Ereignisse aufgetreten sind.

Die unten stehende Tabelle zeigt mögliche Statussymbole an.

TABELLE 9-4. Anti-Spam-Statussymbole

STATUSSYMBOL	BESCHREIBUNG
	Achtung. Spam-Nachrichten umfassen 10 % oder mehr der gesamten vom Exchange Server verarbeiteten Nachrichten (Client Server Messaging/Worry-Free Business Security Advanced, standardmäßig). Administratoren können den Grenzwert auf dem verwalteten Server ändern.
	Das Symbol wird nicht verwendet, um diese Details anzuzeigen.

Details des Netzwerkvirenstatus

Der Bereich zu Details des Netzwerkvirenstatus enthält Warnungen vor kritischer Netzwerkvirenaktivität im Netzwerk. In der Ereignisverwaltung wird mit Statussymbolen und Farbcodierungen angezeigt, ob die Netzwerkvirenaktivität in Kundendomänen einen bestimmten Grenzwert erreicht hat. Ein Netzwerkvirenereignis wird auf dem Dashboard nur dann angezeigt, wenn ein oder mehrere Netzwerkvirenereignisse auftreten.

TABELLE 9-5. Netzwerkvirenstatussymbole

STATUSSYMBOL	BESCHREIBUNG
	Hierbei handelt es sich um eine Warnmeldung. Zehn oder mehr Netzwerkvirenvorfälle innerhalb einer Stunde gefunden (Worry-Free Business Security (alle), Standard). Administratoren können den Grenzwert auf dem verwalteten Server ändern. Das Einstundenintervall ist der 60-Minuten-Zeitraum vor dem Bewertungszeitpunkt.
	Das Symbol wird nicht verwendet, um diese Details anzuzeigen.

Greifen Sie auf weitere Informationen oder Aktionen – sofern verfügbar – zu, indem Sie auf **Details** klicken.

Details des Web-Reputation-Status

Web Reputation bewertet das potenzielle Sicherheitsrisiko angeforderter Webseiten, bevor diese angezeigt werden. Je nach Bewertung durch die Datenbank und der konfigurierten Sicherheitsstufe verweigert oder erlaubt der Client/Server Security Agent die Anfrage auf Computern, die von Worry-Free Business Security (alle) verwaltet werden. Der Abschnitt zu den Web Reputation Services informiert über die Anzahl der Versuche, Webseiten herunterzuladen, die als Sicherheitsrisiko eingestuft wurden. Ein Web-Reputation-Ereignis wird auf dem Dashboard nur dann angezeigt, wenn ein oder mehrere Web-Reputation-Ereignisse aufgetreten sind.

TABELLE 9-6. Web-Reputation-Statussymbole

STATUSSYMBOL	BESCHREIBUNG
	Die Clients melden zahlreiche oder häufige URL-Verstöße. Innerhalb einer Stunde wurden mehr als 200 Verstöße gefunden (Worry-Free Business Security (alle), Standard). Administratoren können den Grenzwert auf dem verwalteten Server ändern. Das Einstundenintervall ist der 60-Minuten-Zeitraum vor dem Bewertungszeitpunkt.
	Das Symbol wird nicht verwendet, um diese Details anzuzeigen.

Details des Verhaltensüberwachungsstatus

Die Verhaltensüberwachung überwacht, ob ein Client versucht, das Betriebssystem und andere Programme zu ändern. Wenn ein Client/Server Security Agent auf Computern, die von Worry-Free Business Security (alle) verwaltet werden, einen solchen Versuch entdeckt, wird der Benutzer vom Security Agent über die Änderung benachrichtigt. Der Benutzer hat die Möglichkeit, die Anfrage zuzulassen oder zu sperren. Worry-Free Business Security (alle) Administrators (oder Benutzer) können Ausschlusslisten erstellen, um bestimmte Programme trotz Verstoß gegen eine überwachte Änderung auszuführen oder bestimmte Programme vollständig zu sperren. Übersteigt die Anzahl der Verstöße den Schwellenwert, ändert sich das Statussymbol und die Anzahl der Vorfälle wird auf dem **Dashboard** und im Fenster **Ereignisverwaltung** angezeigt.

TABELLE 9-7. Web-Reputation-Statussymbole

STATUSSYMBOL	BESCHREIBUNG
	Die Clients melden zahlreiche oder häufige URL-Verstöße. Innerhalb einer Stunde wurden mehr als 200 Verstöße gefunden (Worry-Free Business Security (alle), Standard). Administratoren können den Grenzwert auf dem verwalteten Server ändern. Das Einstundenintervall ist der 60-Minuten-Zeitraum vor dem Bewertungszeitpunkt.
	Das Symbol wird nicht verwendet, um diese Details anzuzeigen.

Details des URL-Filter-Status

Das URL-Filter-Modul bietet leistungsstarke, effektive Tools, um den Internet-Zugriff der Mitarbeiter zu verwalten und anstößige oder nicht arbeitsbezogene Websites zu blockieren. Der URL-Filter filtert Inhalte mit Hilfe einer Datenbank, die Millionen kategorisierter URLs enthält, und verwendet eine dynamische Bewertungstechnologie, um neue Webseiten zu klassifizieren – in Echtzeit oder im Hintergrund. IT-Manager können URL-Richtlinien nach Gruppe oder Benutzer, Kategorie, Dateityp, Uhrzeit, Tag, Bandbreite und anderen Variablen festlegen.

Hinweis

URL-Filter gelten nur für Worry-Free Business Security Services und Worry-Free Business Security Standard und Advanced Versionen 6.0 und höher.

TABELLE 9-8. URL-Filter-Statussymbole

STATUSSYMBOL	BESCHREIBUNG
	Achtung. Mehr als 300 URL-Filter-Ereignisse in der letzten Stunde.
	Das Symbol wird nicht verwendet, um diese Details anzuzeigen.

Details der Gerätesteuerung

Das Gerätesteuerungsmodul bietet leistungsstarke, effektive Tools, um den Zugriff auf externe Speichergeräte und Netzwerkressourcen zu regulieren.

Hinweis

Gerätesteuerung gilt nur für Worry-Free Business Security Standard und Worry-Free Business Security Advanced Versionen 7.x und höher.

TABELLE 9-9. Statussymbole der Gerätesteuerung

STATUSSYMBOL	BESCHREIBUNG
	Achtung. Mehr als 300 nicht autorisierte Gerätezugriffe in der letzten Stunde.
	Das Symbol wird nicht verwendet, um diese Details anzuzeigen.

Smart Scan

Trend Micro™ Worry-Free Business Security verwendet eine neue Technologie mit dem Namen Smart Scan. Früher verwendeten Worry-Free Business Security Services Clients nur die herkömmliche Suche, wobei jeder Client suchrelevante Komponenten herunterladen musste, um eine Suche auszuführen. Beim Prozess mit Smart Scan verwendet der Client stattdessen die Pattern-Datei, die sich auf dem Smart Scan Server befindet. Es werden nur die Ressourcen des Smart Protection Server für das Durchsuchen von Dateien verwendet.

Hinweis

Die Smart Protection-Technologie wird von Worry-Free Business Security Standard und Worry-Free Business Security Advanced Versionen 6.x und höher, und nur von Worry-Free Business Security Services 3.x und höher verwendet.

TABELLE 9-10. Statussymbole zur Speichernutzung

STATUSSYMBOL	BESCHREIBUNG
	Der Smart Protection Service wurde auf einem Worry-Free Business Security Agent unterbrochen.
	Der Smart Protection Service wurde auf einem Worry-Free Business Security Agent unterbrochen.

Wenn der Smart Protection Service nicht ausgeführt wird, warten Sie 30 Minuten, damit der Agent genügend Zeit für die Synchronisierung mit dem Global Scan Server hat. Wenn der Agent immer noch keine Verbindung zum Global Scan Server aufbaut, überprüfen Sie die Internet-Verbindung des Agents. Weiteren Support erhalten Sie von Ihrem Support-Anbieter.

Komponenten-Update

Die folgende Tabelle zeigt die Symbole, die auf der Seite **Kunde** zur Anzeige von Update-Problemen verwendet werden.

TABELLE 9-11. Update-Statussymbole

STATUSSYMBOL	BESCHREIBUNG
	Achtung. Dieses Statussymbol wird unter einer der folgenden Bedingungen angezeigt: • Das verwaltete Produkt wurde seit über sieben Tagen nicht mehr aktualisiert. • Die Verteilungsrate für Pattern und Engine auf Desktop-PCs und Servern beträgt weniger als 90%.

Statussymbol	Beschreibung
	Aktion erforderlich. Dieses Statussymbol wird unter einer der folgenden Bedingungen angezeigt: • Das verwaltete Produkt wurde seit über 14 Tagen nicht mehr aktualisiert. • Die Verteilungsrate für Pattern und Engine auf Desktop-PCs und Servern beträgt weniger als 70%. • Mindestens ein Exchange Server ist ohne aktuelle Sicherheitskomponenten.

Um Update-Probleme zu beheben, wechseln Sie zu **Kunden** > **{Kunde}** > **System** > **Komponenten-Update** > **{Produkttyp}**, wählen Sie das Produkt/den Service aus und klicken Sie auf **Lösen**.

Nachdem Sie den verwalteten Server erfolgreich aktualisiert und die aktuellen Komponenten verteilt haben, sollten Sie eine manuelle Suche (unter dem Menü**Aktionen**) durchführen. Die Suche entdeckt Bedrohungen, die von veralteten Komponenten nicht gefunden wurden.

Speichernutzung

Auf der Seite **Kunden** können Sie mit Hilfe der Symbole mögliche und tatsächliche Probleme mit dem Festplattenspeicher erkennen und die aktuelle Festplattennutzung überwachen. Diese Symbole werden in der folgende Tabelle beschrieben.

Tabelle 9-12. Statussymbole zur Speichernutzung

Statussymbol	Beschreibung
	Das Symbol wird nicht verwendet, um diese Details anzuzeigen.
	Aktion erforderlich. Dieses Statussymbol wird angezeigt, wenn mehr als ein Computer weniger als 1 % Festplattenspeicher zur Verfügung hat (1 % ist der Standard von Worry-Free Business Security Standard und Worry-Free Business Security Advanced, der über die Worry-Free Business Security Standard Konsole und Worry-Free Business Security Advanced Konsole geändert werden kann).

Wenden Sie sich bei Problemen in Zusammenhang mit der Speichernutzung an den Administrator der betroffenen Domäne.

Kapitel 10

Berichte

Dieser Abschnitt enthält die folgenden Themen:

- *Überblick über Berichte auf Seite 10-2*
- *Berichte erstellen auf Seite 10-3*
- *Berichte anzeigen auf Seite 10-7*
- *Berichte bearbeiten auf Seite 10-7*
- *Berichte herunterladen und versenden auf Seite 10-7*
- *Berichte abonnieren auf Seite 10-8*

Überblick über Berichte

Trend Micro Remote Manager ermöglicht das Erstellen, Herunterladen und automatische Senden von Berichten. Berichte bieten einen Überblick über Lizenzstatus, Bewertungsergebnisse, Bedrohungsvorfälle, wichtige Bedrohungen sowie die am stärksten betroffenen Computer, Dateien und E-Mail-Adressen in den Netzwerken Ihrer Kunden.

Berichte enthalten eine Reihe statistischer Angaben zu Worry-Free Business Security (alle) und Hosted Email Security. Remote Manager berücksichtigt Berichtprofile, zeitgesteuerte Berichte und Einzelberichte, Datumsbereiche und mehrere E-Mail-Empfänger. Remote Manager speichert die 30 neuesten Tagesberichte, zehn neuesten Wochenberichte und fünf neuesten Monatsberichte. Allgemeine Berichte eignen sich für Reseller und Kunden. Detaillierte Berichte eignen sich für Reseller und Partner.

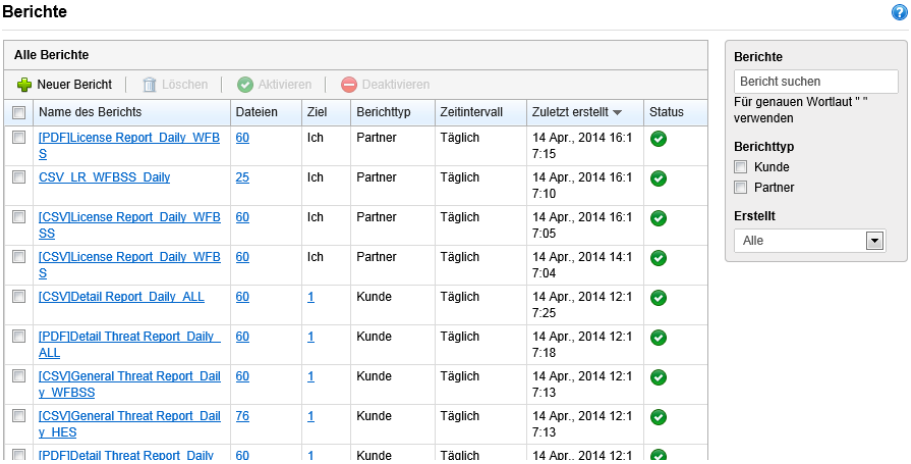


ABBILDUNG 10-1. Die Seite "Berichte"

Über Berichtprofile können Sie mehrere Berichte aus einem einzigen Profil erstellen. Sie können beispielsweise einen Einzelbericht für den heutigen Tag festlegen und erstellen und morgen einige Optionen ändern und den Bericht recyceln, ohne den gesamten Bericht erneut zu erstellen. Mit dem Remote Manager können Sie derzeit allgemeine und detaillierte Berichte erstellen.

Berichte erstellen

Trend Micro Remote Manager bietet folgende Möglichkeiten, um eine Berichtvorlage zu erstellen:

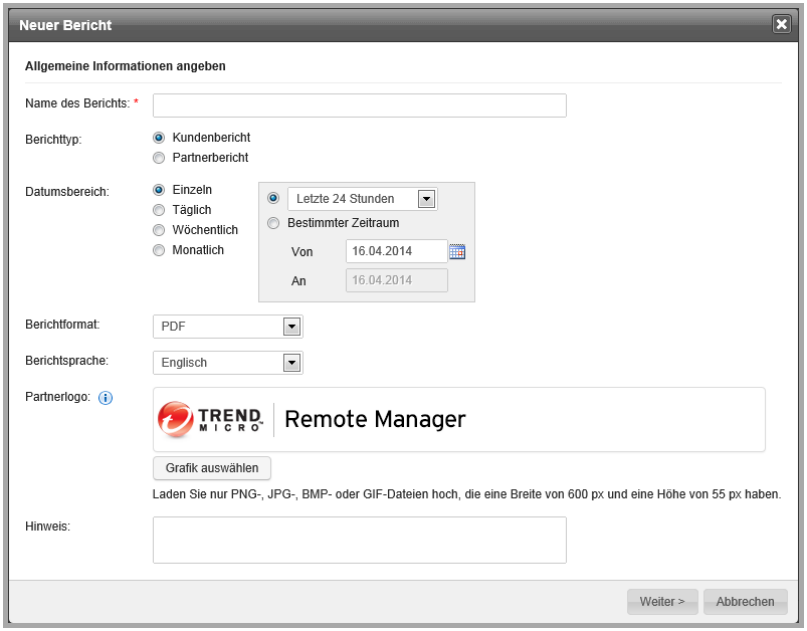
- Klicken Sie auf einen vorhandenen Bericht, bearbeiten Sie ihn, und klicken Sie am unteren Rand des Fensters auf **Speichern**.
- Erstellen Sie eine neue Berichtvorlage. Weitere Informationen finden Sie unter *Berichtvorlagen erstellen auf Seite 10-3*.

Berichtvorlagen erstellen

Prozedur

1. Klicken Sie auf **Berichte** > **Neuer Bericht**.

   Das Fenster **Neuer Bericht** wird angezeigt.



2. Aktualisieren Sie auf Anforderung folgende Einstellungen:

   - **Name des Berichts**
   - **Berichttyp**: Weitere Informationen finden Sie unter *Überblick über Berichte auf Seite 10-2*.

   Nur Worry-Free Business Security bietet einen ausführlichen Bericht.

3. Wählen Sie den **Berichtszeitraum**:

   - **Einzelbericht**

Optionen	Beschreibung
Heute	Verwendet die zwischen Mitternacht bis zum Zeitpunkt der Berichterstellung empfangenen Daten (angepasst für die ausgewählte Zeitzone). **Hinweis** Die Zeitzone, die im Bericht angezeigt wird, entspricht der vom Reseller ausgewählten Zeitzone bei der Profilerstellung. Sie wird nicht durch den Kundencomputer festgelegt.
Letzte 7 Tage	Verwendet zur Berichterstellung die in den letzten 7 Tagen empfangenen Daten (mit Ausnahme der Daten des aktuellen Tages).
Letzte 30 Tage	Verwendet zur Berichterstellung die in den letzten 30 Tagen empfangenen Daten (mit Ausnahme der Daten des aktuellen Tages).
Bestimmter Zeitraum	Das Datum "Von" muss nach dem ersten Datum des letzten Monats liegen oder damit identisch sein (Remote Manager speichert nur die Daten des vergangenen und aktuellen Monats). Das Datum "Bis" darf nicht nach dem aktuellen Datum liegen.

   - **Regelmäßiger Bericht**

Optionen	Beschreibung
Tagesbericht	Das Enddatum muss nach dem aktuellen Datum liegen, damit für jeden Tag im festgelegten Zeitraum ein Bericht auf Grundlage der Daten des vorangegangenen Tages erzeugt wird. Wurde beispielsweise ein Zeitraum vom 27. bis zum 29. Januar 2009 festgelegt, wird: • Am 27. Januar ein Bericht basierend auf dem 26. Januar erstellt • Am 28. Januar ein Bericht basierend auf dem 27. Januar erstellt • Am 29. Januar ein Bericht basierend auf dem 28. Januar erstellt
Wochenbericht	Remote Manager erstellt den Wochenbericht jeden Montag anhand der Daten der vorherigen Woche. Das bedeutet, dass zum Erstellen eines Berichts für die aktuelle Woche als Enddatum mindestens der Montag der Folgewoche festgelegt werden muss.
Monatsbericht	Remote Manager erstellt den Monatsbericht am zweiten Tag jedes Monats anhand der Daten des Vormonats. Das bedeutet, dass zum Erstellen eines Berichts für den aktuellen Monat als Enddatum mindestens der zweite Tag des Folgemonats festgelegt werden muss.

4. Legen Sie den **Berichtinhalt** fest. Dies umfasst die folgenden Berichtformatelemente:

Option	Bezeichnung
Berichtformat	PDF- oder CSV-Format
Berichtsprache	Die Sprache des Berichts.
Logo	Das Logo ist optional. Es sollte eine `PNG`-, `JPG`-, `BMP`- oder `GIF`-Partnerlogografik mit einer empfohlenen Größe von 600 (Breite) und 55 (Höhe) Pixeln verwendet werden.

OPTION	BEZEICHNUNG
Hinweis	Das Hinweisfeld ist für interne Zwecke und wird auf dem Bericht selbst nicht angezeigt.

5. Klicken Sie auf **Weiter**.

6. Wählen Sie die Daten für den Bericht aus. Wählen Sie eine Berichtsvorlage aus sowie die Daten, die erstellt werden sollen.

Hinweis

Wenn der Reseller nicht mit dem Server des Kunden verbunden ist oder keine Daten vorliegen, werden für den Kunden keine Informationen angezeigt.

7. Klicken Sie auf **Weiter**.

8. Wählen Sie die Kunden aus, die diesen Bericht erstellen.

Hinweis

Sie können auf **Fertig** klicken. Die Berichte werden für die ausgewählten Kunden erstellt.

9. Geben Sie die Details für die E-Mail-Berichte an. Die in den E-Mail-Optionen angegebenen **Empfänger** werden über die Kontaktliste der Unternehmen ermittelt. Sie können auch eine E-Mail-Adresse hinzufügen, an die die erstellten Berichte gesendet werden.

Hinweis

Für jeden ausgewählten Kunden sind andere E-Mail-Empfänger angegeben. Sie können E-Mail-Empfänger oder ein Logo je nach Kunde löschen.

10. Klicken Sie auf **Fertig**.

Remote Manager fügt die Berichtvorlage zur Liste der Berichtvorlagen hinzu.

Berichte anzeigen

Ein Bericht muss mindestens einmal erstellt worden sein, um ihn anzeigen zu können.

Gehen Sie zu **Berichte** > **{Berichtsname}** > **Berichtdateien (Registerkarte)** > **{Datei unter "Ansicht"}**.

Weitere Informationen finden Sie unter *Überblick über Berichte auf Seite 10-2*.

Berichte bearbeiten

Gehen Sie zu **Berichte** > **{Berichtsname}**.

Weitere Informationen finden Sie unter *Berichtvorlagen erstellen auf Seite 10-3*.

Berichte herunterladen und versenden

Sie können Berichte herunterladen und an Empfänger versenden. Die Liste der Empfänger wird festgelegt, wenn der Bericht erstellt wird, kann aber später geändert werden.

Prozedur

1. Gehen Sie zu **Berichte** > **{Element oder Anzahl der Elemente unter "Berichtdateien"}** > **{Bericht unter "Ansicht"}**.
2. Wählen Sie die Berichte aus, die Sie versenden oder herunterladen möchten.
3. Klicken Sie auf **Send (Senden)** oder **Download**.

   Weitere Informationen finden Sie unter *Berichte abonnieren auf Seite 10-8*.

Berichte abonnieren

Prozedur

1. Gehen Sie zu **Berichte** > **{Berichtsname}** > **Zielpublikum (Registerkarte)** > **Ziel hinzufügen**.
2. Wählen Sie den Kundenbericht aus.

   Hinweis

   Die Liste der E-Mail-Empfänger wird beim Erstellen von Berichten anhand der Kontaktdaten generiert.

3. Ändern Sie die Betreffzeile nach Bedarf.
4. Klicken Sie auf **Speichern**.

Kapitel 11

Fehlerbehebung und bekannte Probleme

Dieser Abschnitt enthält die folgenden Themen:

- *Fehlerbehebung in der Trend Micro Remote Manager Web-Konsole auf Seite 11-2*
- *Fehlerbehebung für den Agent auf Seite 11-6*
- *Bekannte Probleme mit dem Server auf Seite 11-11*
- *Bekannte Probleme mit dem Agent auf Seite 11-14*
- *Häufig gestellte Fragen auf Seite 11-15*

Fehlerbehebung in der Trend Micro Remote Manager Web-Konsole

Dieser Abschnitt enthält die folgenden Themen:

Zugriffsprobleme

Ein Benutzer kann sich nicht bei Trend Micro Remote Manager anmelden.

Lösung

Für dieses Problem gibt es zwei mögliche Gründe:

- Im Browser ist JavaScript deaktiviert. Remote Manager erfordert, dass diese Option aktiviert ist. Weitere Hinweise finden Sie in der Dokumentation zu Ihrem Browser.
- Das Profil wurde nicht synchronisiert. Wenn Sie sich gerade eben bei der Trend Micro Licensing Management Platform registriert haben und sich nicht anmelden können, warten Sie einige Minuten, bis die Informationen synchronisiert werden.

Domänenansicht nach Installation des Agents nicht sichtbar

Nach Installation des Remote Manager Agents auf dem verwalteten Server wird die Domain-Ansicht nicht in der Konsole angezeigt.

- Die GUID (Globally Unique Identifier) ist falsch.
- Der Remote Manager Agent kann nicht mit Remote Manager kommunizieren.

Lösung

1. Vergewissern Sie sich, dass die eingegebene GUID korrekt ist.
    a. Verwenden Sie einen Texteditor, wie Notepad, um `C:\Programme\Trend Micro\WFRMAgentForCSM\AgentSysConfig.xml` auf dem Security Server zu öffnen.

b. Überprüfen Sie die GUID direkt nach dem Parameter.

c. Speichern Sie nach Korrektur der GUID die Datei, und starten Sie den Trend Micro Remote Manager Agent Dienst neu.

d. Prüfen Sie nach ein paar Minuten den Status der Kunden-Domain auf dem Remote Manager.

2. Prüfen Sie die Agent-Server-Verbindung über die Funktion Verbindung testen.

   a. Navigieren Sie zu **Start** > **Programme** > **Trend Micro Remote Manager Agent** > **Agent-Konfigurationstool**.

   b. Klicken Sie auf **Verbindung testen**.

   c. Falls die Testverbindung fehlschlägt:

      i. Prüfen Sie, ob der verwaltete Server eine Internet-Verbindung herstellen kann.

      ii. Prüfen Sie, ob Sie die Trend Micro Remote Manager Serveradresse korrekt eingegeben haben.

      iii. Verbindet sich der Security Server über einen Proxy-Server mit dem Internet, müssen auch die Einstellungen des Proxy-Servers angegeben werden.

Knoten in Struktur kann nicht erweitert werden

Wenn ein Knoten in der Domänenstruktur (auf der Registerkarte **Kunden**) beim Anklicken nicht erweitert wird, sind Gruppen- und Client-Informationen auf dem Worry-Free Business Security Server und dem Trend Micro Remote Manager Server möglicherweise nicht synchronisiert.

Lösung

Klicken Sie mit der rechten Maustaste auf den Knoten und anschließend auf **Aktion** > **Mit verwaltetem Server synchronisieren**, um Daten erneut vom Agent zum Trend Micro Remote Manager Server zu senden.

Seite kann nicht angezeigt werden

Beim Versuch, die Trend Micro Remote Manager Server-URL zu öffnen, erhalten Sie die Meldung `Die Seite kann nicht angezeigt werden`. Mögliche Ursachen:

- Die Adresse ist falsch.
- Die URL des Trend Micro Remote Manager Servers ist keine vertrauenswürdige Site in Internet Explorer.

Lösung

1. Stellen Sie sicher, dass die URL des Trend Micro Remote Manager Servers eine vertrauenswürdige Sie in Internet Explorer ist.
   a. Öffnen Sie Internet Explorer.
   b. Klicken Sie auf **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Site** > **Sites**.
   c. Prüfen Sie, ob der URL des Trend Micro Remote Manager Servers in der Liste aufgeführt ist. Falls nicht, geben Sie sie ein, und klicken Sie auf **OK**.

Fehlerhafte Informationen auf dem Dashboard

Wenn Sie auf dem Dashboard Informationen über bestimmte Domänen erhalten, die Ihnen falsch oder unvollständig erscheinen.

Lösung

- Überprüfen Sie, ob der verwaltete Server gestartet wurde.
- Überprüfen Sie, ob der Agent gestartet wurde und ordnungsgemäß ausgeführt wird.
  - Prüfen Sie die Angaben in der Remote Manager Web-Konsole unter **Kunden (Registerkarte)** > **Alle Kunden (in der Struktur)** > **{Kunde}** > **WFBS-S/ WFBS-A** > **Server-/Agent-Details (rechter Fensterbereich)** > **Details zum TMRM Agent** (siehe *Agent-Status auf Seite 6-2*).

- Überprüfen Sie den Status des Agents auf dem verwalteten Server (siehe *Agents über den verwalteten Server verwalten auf Seite 6-6*, *Agent-Status auf Seite 6-2* und *Agent-Installation überprüfen auf Seite 4-11*).

- Überprüfen Sie, ob der Kunde den Agent erneut installiert hat. Überprüfen Sie ebenfalls, ob der Kunde den Agent neu installiert und eine andere oder doppelte GUID verwendet hat. Standardmäßig sollte der Agent maximal Daten aus den vergangenen drei Tagen vom verwalteten Server erhalten.

- Sie können versuchen, eine neue GUID zu erzeugen und den Agent neu zu installieren.

Es können keine Befehle übermittelt werden

Wenn Sie keine Netzwerkbefehle an einen Agent übermitteln können.

Lösung

- Worry-Free Business Security Standard oder Worry-Free Business Security Advanced Service wird ausgeführt.

- Client-Agent wird ausgeführt. Falls nicht, starten Sie den Agent neu (siehe *Agent-Dienst auf Seite 4-11*).

- Ports 80 und 443 sind offen. Sie können dies durch einen Telnet-Test vom Remote Manager Server zu den Agents auf Ports 80 und 443 und umgekehrt prüfen. Falls die Ports nicht offen sind, muss der Administrator beim Kunden die Ports auf der internen Firewall öffnen.

Agent-Status ist ungewöhnlich

Ein ungewöhnlicher Agent-Status kann mehrere Gründe haben.

Lösung

1. Der Agent-Status ist ungewöhnlich, wenn der Agent vor dem Herunterfahren keine Abmeldeanfrage an den Remote Manager Server gesendet hat. Starten Sie den Agent-Dienst neu, um dieses Problem zu beheben (siehe *Agent-Dienst auf Seite 4-11*).

2. Sollte das Problem dadurch nicht behoben werden, starten Sie das Agent-Konfigurationstool durch Klicken mit der rechten Maustaste auf das Agent-Symbol, und klicken Sie auf **Konfigurieren**. Klicken Sie auf die Schaltfläche **Verbindung testen**, um die Verbindung des Netzwerks mit dem Remote Manager Server zu testen.

3. Im Falle einer Fehlermeldung überprüfen Sie Ihre Firewall-Richtlinie.

4. Wenn eine Verbindung besteht, überprüfen Sie das Agent-Protokoll (siehe *Speicherorte der Agent-Protokolle und -Konfigurationsdateien auf Seite 6-15*).

5. Wenn das Problem kritisch ist und auch nach dem Neustart des Agent-Dienstes weiter besteht, aktivieren Sie das Fehlerprotokoll (siehe *Das Agent-Fehlerprotokoll aktivieren auf Seite 6-15*), und wenden Sie sich an Ihren Supportanbieter.

Agent funktioniert unter Verwendung einer vorhandenen GUID nicht ordnungsgemäß nach ...

Warum funktioniert der Agent mit einer vorhandenen GUID nicht ordnungsgemäß, nachdem ich das Betriebssystem neu installiert, den Remote Manager Agent neu installiert, die Netzwerkkarte des Computers ausgetauscht oder den Agent auf einem anderen Computer installiert habe?

Lösung

Bevor Sie eine der oben genannten Aktionen durchführen, muss der Agent deinstalliert werden, um vorhandene Daten auf dem Remote Manager Server zu löschen. Der Agent kann sonst mit einer vorhandenen GUID nicht ordnungsgemäß ausgeführt werden.

Fehlerbehebung für den Agent

Probleme mit dem Agent

Wenn Sie die Maus über das Task-Leistensymbol bewegen, wird in einer Statusmeldung angezeigt, ob der Agent ordnungsgemäß funktioniert oder nicht.

TABELLE 11-1. Statusmeldungen des Agent-Taskleistensymbols

NACHRICHT	BESCHREIBUNG
Es ist ein unbekannter Fehler aufgetreten. Überprüfen Sie das System, oder starten Sie den Agent neu.	Es ist ein unbekannter Fehler aufgetreten. Überprüfen Sie das System, oder starten Sie den Agent neu. Unerwartete Fehler (in der Regel Systemfehler) verhindern die ordnungsgemäße Ausführung des Agents. Lösung: Überprüfen Sie, ob auf dem verwalteten Server genügend Speicherplatz zur Verfügung steht oder ob andere Systemprobleme bestehen.
Die Registrierung beim externen Server ist fehlgeschlagen.	Die eingegebene GUID ist möglicherweise ungültig, oder es gibt ein Netzwerkproblem. Lösung Hierfür kann es zwei Ursachen geben: • Prüfen Sie, ob Sie die richtige GUID verwendet haben. Überprüfen Sie mit Hilfe der *Agent-GUID auf Seite 4-8*, welche GUID für die Remote Manager Web-Konsole verwendet werden soll, und überprüfen Sie unter *Die Registrierung beim externen Server ist fehlgeschlagen auf Seite 11-9*, welche GUID der Agent verwendet. Ändern Sie die GUID gegebenenfalls. • Bei einem Netzwerkproblem kann sich der Agent nicht mit dem Server verbinden. Überprüfen Sie die Netzwerkverbindung zwischen dem Worry-Free Business Security (Standard und Advanced) Server und dem Trend Micro Remote Manager Server.
Die Verbindung mit dem externen Server ist fehlgeschlagen.	Der verwaltete Server hat möglicherweise Probleme mit der Internet-Verbindung. Lösung Prüfen Sie die Internet-Verbindung auf dem verwalteten Server. Prüfen Sie ebenfalls die Proxy-Einstellungen des Agents sowie Serveradresse und Port.

NACHRICHT	BESCHREIBUNG
Agent von Remote Manager deaktiviert.	Der Agent wurde über die Remote Manager Web-Konsole vorübergehend deaktiviert. Lösung Aktivieren Sie den Agent über die Remote Manager Web-Konsole.
Der Agent stimmt nicht mit der Client Server Messaging Security (CSM) Version überein.	Die Versionen von Client Server oder Client Server Messaging Security Suite und Agent stimmen nicht überein. Lösung Upgraden Sie den Client Server oder Client Server Messaging Security Suite Server auf die neueste Version und installieren Sie den neuesten Agent.
Agent-Dienst beendet.	Der Agent wurde von Remote Manager abgemeldet. Lösung Starten Sie den Agent-Dienst, indem Sie mit der rechten Maustaste auf das Task-Leistensymbol klicken und **Dienst starten** wählen.
Komponenten konnten nicht geladen werden. Der Agent muss eventuell neu gestartet werden.	Beim Laden einiger Agent-Komponenten sind Probleme aufgetreten. Lösung Versuchen Sie zuerst, den Agent-Dienst neu zu starten, indem Sie mit der rechten Maustaste auf das Task-Leistensymbol klicken und **Dienst neu starten** oder **Dienst starten** wählen. Wenn dies nicht funktioniert, deinstallieren Sie den Agent, und installieren Sie ihn neu. Stellen Sie sicher, dass Sie die gleiche GUID verwenden.

Es konnte keine Verbindung zum Server hergestellt werden

Wenn Sie auf die Schaltfläche "Verbindung testen" im Trend Micro Remote Manager Agent-Konfigurationstool klicken und `Es konnte keine Verbindung zum Server hergestellt werden. Die Einstellungen sind`

möglicherweise ungültig. Geben Sie gültige Einstellungen ein, und versuchen Sie es erneut. angezeigt wird.

Lösung

Versuchen Sie es mit einer der folgenden Abhilfen:

- Der verwaltete Server kann sich nicht mit dem Internet verbinden. Stellen Sie sicher, dass Worry-Free Business Security Advanced Zugriff auf das Internet hat.
- Der FQDN von der Adresse des Remote Manager Kommunikationsservers ist ungültig. Verwenden Sie den FQDN für Ihre Region:
  - Asiatisch-pazifischer Raum: rm-apaca.trendmicro.com
  - Europa und Naher Osten: rm-emeaa.trendmicro.com
  - Japan: rm-jpa.trendmicro.com
  - Lateinamerika: rm-lara.trendmicro.com
  - Nordamerika: rm-usa.trendmicro.com
- Falls sich der Security Server über einen Proxy-Server mit dem Internet verbindet, stellen Sie sicher, dass die Proxy- und Benutzerauthentifizierungseinstellungen korrekt konfiguriert sind.

Die Registrierung beim externen Server ist fehlgeschlagen

Beim Bewegen der Maus über das Symbol des Trend Micro Remote Manager Agents wird Die Registrierung beim externen Server ist fehlgeschlagen angezeigt.

Lösung

Dies weist auf eine falsche GUID (Globally Unique Identifier) hin. Problemlösung:

1. Fahren Sie mit <install path>\Trend Micro\WFRMAgentForCSM fort.
2. Öffnen Sie die Datei AgentSysConfig.xml in einem Texteditor.

3. Suchen Sie die GUID zwischen den Parametern "<AgentGUID>" und "</AgentGUID>".
4. Bearbeiten Sie die GUID, und speichern Sie die Datei.
5. Öffnen Sie die Datei csmSysConfig.xml im selben Ordner mit einem Texteditor.
6. Suchen Sie die GUID zwischen den Parametern "<ProductGUID>" und "</ProductGUID>".
7. Bearbeiten Sie die GUID, und speichern Sie die Datei.
8. Klicken Sie mit der rechten Maustaste auf das Symbol des Trend Micro Remote Manager Agents in der Task-Leiste, und klicken Sie auf **Dienst neu starten**.

Verbindungsprobleme mit Hosted Email Security

Wenn Sie keine Verbindung mit Hosted Email Security herstellen oder diese Verbindung nicht trennen können, wird unten auf der Seite eine der folgenden Meldungen angezeigt:

MELDUNGEN	LÖSUNG
Es konnte keine Verbindung zum Remote Manager Server hergestellt werden. Überprüfen Sie die Netzwerkverbindung und den Status des Remote Managers.	Überprüfen Sie danach die Netzwerkverbindung und den Status des Remote Managers erneut.
Ungültiger Autorisierungsschlüssel	Überprüfen Sie die GUID. Wenn die GUID ungültig ist, löschen Sie den Agent und versuchen Sie erneut, eine Verbindung herzustellen.
Autorisierungsschlüssel duplizieren	Überprüfen Sie die GUID. Wenn die GUID ungültig ist, löschen Sie den Agent und versuchen Sie erneut, eine Verbindung herzustellen.

MELDUNGEN	LÖSUNG
Es kann keine Verbindung zum Remote Manager Remote Manager Server hergestellt werden. Überprüfen Sie die Netzwerkverbindung und den Status des Remote Manager Servers.	Überprüfen Sie die Netzwerkverbindung und den Status des Remote Managers, versuchen Sie es dann erneut.
Interner Server-Fehler	Wenden Sie sich an Ihren Supportanbieter.

Bekannte Probleme mit dem Server

In dieser Version sind folgende Probleme mit dem Server bekannt.

Inkonsistente Statussymbole

Während der ersten Datenerfassung (direkt nach der Registrierung des Agents beim Server) zeigt Remote Manager möglicherweise Virenschutz- und Anti-Spam-Statussymbole an, die mit der angezeigten Anzahl von Viren- und Spam-Vorfällen nicht übereinstimmen.

Direkt nach der Registrierung beim Server übermittelt der Agent den aktuellen Virenschutz- und Anti-Spam-Status von Worry-Free Business Security (alle), aber nicht die Verlaufsdaten, auf denen dieser Status beruht. Daher kann beispielsweise ein rotes Statussymbol ohne Vorfälle angezeigt werden.

Lösung

Remote Manager zeigt das korrekte Symbol und die korrekten Daten an, sobald Worry-Free Business Security (alle) einen Vorfall entdeckt.

Spam-Daten inkonsistent mit Worry-Free Business Security Standard oder Advanced

Die Spam-Daten bei Worry-Free Business Security Standard oder Worry-Free Business Security Advanced und Remote Manager können unterschiedlich sein, wenn sich die Server der beiden Systeme in verschiedenen Zeitzonen befinden.

Lösung

Spam-Vorfälle in der Remote Manager Web-Konsole und Berichte können je nach Zeitunterschied zwischen den Servern ein früheres oder späteres Datum aufweisen.

Falscher Benutzername in der Worry-Free Business Security Services-Konsole

Nach dem Anmelden bei Worry-Free Business Security Services über die Remote Manager Web-Konsole wird auf der Worry-Free Business Security Services-Konsole der Name des Resellers und nicht der Name des Worry-Free Business Security Services-Kunden angezeigt.

Lösung

Für dieses Problem gibt es derzeit keine Lösung.

Inkonsistente Lizenzinfo in der Worry-Free Business Security Services-Konsole

Wenn ein Reseller als Reaktion auf ein Lizenzereignis die Lizenzinformationen in der Remote Manager Web-Konsole bearbeitet, bleibt die Warnung bestehen, bis Worry-Free Business Security Services sich mit Remote Manager synchronisiert.

Lösung

Warten Sie ca. fünf Minuten, bis Worry-Free Business Security Services sich mit Remote Manager synchronisiert hat.

Gleichzeitige Anmeldungen von zwei Registerkarten/ Fenstern desselben Browsers sind nicht zulässig

Wenn ein Reseller versucht, sich mehr als einmal über eine andere Registerkarte oder ein anderes Fenster desselben Browsers anzumelden, wird der Reseller automatisch zu der offenen Registerkarte oder dem offenen Fenster weitergeleitet.

Lösung

Melden Sie sich von der ersten Sitzung ab, bevor Sie eine neue Sitzung starten.

Ältere Berichte werden automatisch gelöscht

Sie können nur die maximale Anzahl von Tagesberichten ändern, die von Remote Manager gespeichert werden. Wenn diese Anzahl erreicht ist, werden ältere Berichte automatisch gelöscht.

Lösung

Trend Micro empfiehlt, ältere Berichte auf Computer oder andere Speichergeräte herunterzuladen.

Ein abgelaufenes Worry-Free Business Security Services-Konto kann nicht verwaltet werden

Remote Manager zeigt keine Informationen zu abgelaufenen Worry-Free Business Security Services Konten an, da ältere Kontoinformationen von Worry-Free Business Security Services automatisch bereinigt werden.

Lösung

Trend Micro empfiehlt, Worry-Free Business Security Services Konten bei Bedarf zu erneuern.

Unterbrochene ConnectWise-Verbindung

Die ConnectWise-Verbindung mit einem Kunden wird unterbrochen, wenn die Unternehmens-ID in ConnectWise aktualisiert wird.

Lösung

Aktualisieren Sie im Fenster Remote Manager Kunde in ConnectWise die neue Unternehmens-ID.

Bekannte Probleme mit dem Agent

In dieser Version sind folgende Probleme mit dem Agent bekannt.

Erneut installierte Agents liefern überlappende Daten

Nach der Registrierung übermitteln Agents automatisch bestimmte Worry-Free Business Security (alle) Daten für einen Zeitraum von drei Tagen. Wird ein Agent innerhalb von drei Tagen deinstalliert und anschließend erneut installiert, ruft der Agent möglicherweise Daten ab, die mit den abgerufenen Daten vor der Deinstallation überlappen.

Lösung

Sichern Sie die Agent-Konfigurationsdateien vor der Deinstallation des Agents, und stellen Sie diese Dateien nach der Neuinstallation des Agents wieder her. Weitere Informationen finden Sie unter *Agent-Einstellungen sichern und wiederherstellen auf Seite 6-12*.

Ergebnisse des Befehls "Durchsuchen" können nicht überprüft werden

Der Agent kann nicht prüfen, ob Worry-Free Business Security Standard oder Worry-Free Business Security Advanced den Befehl "Durchsuchen" an das Netzwerk verteilt. Remote Manager kann daher die Ergebnisse des Befehls "Durchsuchen" nicht prüfen.

Lösung

Eventuell müssen Sie den Status des Suchbefehls durch den IT-Administrator Ihres Kunden überprüfen lassen.

Agent-Konfigurationstool ist nach dem Upgrade des Agents nicht mehr sichtbar

Das Agent Konfigurationstool ist nach dem Upgrade des Agents auf dem Betriebssystem Vista™ oder Windows Server 2008™ nicht sichtbar. Der Benutzer führt vor dem Upgrade normalerweise das Agent Konfigurationstool unter dem Konto des

Benutzers aus. Beim Upgrade wird das Tool beendet und anschließend von LocalSystem statt dem Konto des Benutzers neu gestartet. Deshalb kann es der Benutzer nicht sehen, obwohl es ausgeführt wird.

Lösung

Der Computer sollte neu gestartet werden, um das Agent Konfigurationstools über das Benutzerkonto neu zu starten.

Häufig gestellte Fragen

Häufig gestellte Fragen zur Webkonsole

Weshalb zeigt der Agent bei einem Remote Manager Server der Version 3.2 weiterhin die Version 1.6 auf der Remote Manager Konsole an?

Remote Manager 3.2 verwendet weiterhin den Agent der Version 1.6 (auf Servern vor WFBS 6.0); nur die Serverversion ist 3.2.

Kann ein Reseller mehr als ein Remote Manager Konto haben?

Nein. Unter Remote Manager 3.1 steht jedem Reseller nur ein Konto zur Verfügung.

Warum ist die Kundenstruktur auch nach Auswahl von Hosted Email Security in der Liste "Anzeigen nach" (oberhalb der Struktur) weiterhin nach Kundennamen sortiert?

Bei der Auswahl von Hosted Email Security werden alle Hosted Email Security Kunden gefiltert; es wird jedoch nicht nach Hosted Email Security sortiert. Mit anderen Worten: Wenn Sie aus dem Listenfeld Hosted Email Security auswählen, werden nur Kunden mit Hosted Email Security angezeigt.

Hinweis

Andere Produkte dieses Hosted Email Security Kunden werden ebenfalls angezeigt.

Warum sind bestimmte Menüelemente oder Optionen abgeblendet?

Bestimmte Menüelemente zum Senden von Befehlen an einen Agent können abgeblendet sein. Dies kann daran liegen, dass der Agent noch nicht am Remote Manager Server registriert ist oder relevante Daten auf Grund von Zeitverzögerungen des Netzwerks oder aus anderen Gründen noch nicht übertragen wurden.

Warum kann ich mein Kennwort auf der Trend Micro Licensing Management Platform nicht ändern?

Möglicherweise wird die Licensing Management Platform gewartet. Warten Sie einige Zeit und versuchen Sie danach erneut, Ihr Kennwort zu ändern. Falls das Problem weiterhin besteht, wenden Sie sich an Ihren Supportanbieter.

Ich habe gerade Daten in der Konsole aktualisiert. Der Status ist jedoch unverändert. Woran könnte das liegen?

Es dauert einige Minuten, bis die Daten über die Services hinweg synchronisiert werden. Beispiele für verzögerte Änderungen sind Aktualisierungen der Lizenz oder Arbeitsplätze, das Zurücksetzen von Zählern usw.

Der Service der Worry-Free Business Security Services wird in der Konsole nicht angezeigt. Warum?

Wenn der Service vor mehr als 60 Tagen abgelaufen ist, wird der nicht aufgeführt.

Ich habe auf den Link geklickt, um mich bei Worry-Free Business Security Services anzumelden. Eine Fehlermeldung wird angezeigt. Warum?

Dies kann vorkommen, wenn Worry-Free Business Security Services wegen Wartungsarbeiten außer Betrieb ist oder ein Problem mit der Licensing Management Platform vorliegt. Warten Sie einige Zeit und klicken Sie danach erneut auf den Link.

Warum ist der Kunde, den ich auf der Licensing Management Platform erstellt habe, in Remote Manager nicht sichtbar?

Es dauert einige Minuten, bis die Daten über die Services hinweg synchronisiert werden.

Warum wird nach dem Klicken auf die Schaltfläche Update weiterhin Alarmstufe Rot für "Nicht mehr aktuelle verwaltete Server" angezeigt?

Die Schaltfläche **Update** sendet nur Befehle an den Worry-Free Business Security Standard oder Worry-Free Business Security Advanced Server. Folgende Probleme können auftreten:

- Der Worry-Free Business Security Standard oder Worry-Free Business Security Advanced Server empfängt den Update-Befehl, kann diesen aber auf Grund der Servereinstellungen nicht ausführen.
- Der Worry-Free Business Security Standard oder Worry-Free Business Security Advanced Server hat ein Server-Update durchgeführt, jedoch wurden dabei die meisten zugehörigen CSAs nicht aktualisiert. Daher wird weiterhin Alarmstufe Rot an Remote Manager gesendet. Es kann einige Zeit dauern, bis die meisten CSAs aktualisiert sind.

Häufig gestellte Fragen zu Hosted Email Security

Warum werden die aktuellen Daten der letzten drei Stunden nicht auf der Seite Live-Status angezeigt?

Auf dem Hosted Email Security Server werden Daten über einen Zeitraum von zwei Stunden erfasst. Um sicherzustellen, dass der Remote Manager Server die Daten vom Hosted Email Security Server integriert hat, verzögert sich die Datenerfassung um drei Stunden.

Warum werden die Funktionen "Mit Server synchronisieren" und "Zur Kundenkonsole wechseln" abgeblendet, wenn man in der Kundenstruktur mit der rechten Maustaste auf "Hosted Email Security" klickt?

Es gibt drei mögliche Ursachen dafür, dass Hosted Email Security nicht aktiv ist.

- Hosted Email Security ist noch nicht mit Remote Manager verbunden.
- Der Kunde hat die Verbindung getrennt. Siehe *Einen Hosted Email Security Kunden mit der Remote Manager Konsole verbinden auf Seite 4-14*.
- Die Kundenansicht muss möglicherweise aktualisiert werden.

Warum erhalte ich die Fehlermeldung "Ihr Hosted Email Security Kunde hat keine Verbindung zu Remote Manager hergestellt oder wurde durch Hosted Email Security getrennt. Wenden Sie sich an Ihren Administrator.", wenn ich versuche, zur Hosted Email Security Konsole des Kunden umzuleiten, nachdem der Kunde eine Verbindung von Hosted Email Security mit Remote Manager hergestellt hat?

Nach Eingabe der GUID oder des Autorisierungsschlüssels und Klicken auf **Verbinden** kann es bis zu zehn Minuten dauern, bis die Verbindung von Hosted Email Security mit der Remote Manager Web-Konsole hergestellt wurde. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.

Warum wird auf der Remote Manager Web-Konsole für den Hosted Email Security Aktivierungscode (AC) und das Ablaufdatum eines Kunden "n. v." angezeigt?

Wenn ein Hosted Email Security Kunde den Hosted Email Security Service nicht mit Remote Manager verbunden hat oder die Verbindung getrennt hat, kann Remote Manager keine Daten abrufen. Es ist auch möglich, dass Hosted Email Security keinen gültigen Aktivierungscode und kein Ablaufdatum für diesen Kunden finden kann. Dieser Fall tritt allerdings selten auf.

Häufig gestellte Fragen zu Berichten

Gibt es eine Begrenzung für die maximale Anzahl von Berichten, die gespeichert werden können?

Ja. Remote Manager begrenzt die Anzahl von gespeicherten Berichten. Wenn diese Anzahl erreicht ist, werden ältere Berichte automatisch gelöscht. Die Anzahl der gespeicherten Berichte ist:

- **Tagesberichte**: Es werden maximal 30 Berichte gespeichert.
- **Wochenberichte**: Es werden maximal 10 Berichte gespeichert.
- **Monatsberichte**: Es werden maximal 5 Berichte gespeichert.

Warum werden Berichte nicht erzeugt?

Überprüfen Sie, ob die Festplatte voll ist. Remote Manager bietet zurzeit nur 512 MB Speicher. Versuchen Sie, einige Berichte auf Ihre lokale Festplatte herunterzuladen, löschen Sie sie von der Konsole und versuchen Sie erneut, die Berichte zu erzeugen.

Warum wird nach der Erstellung eines Profils für einen Einzelbericht im Berichtverlauf kein neuer Bericht erstellt?

Warten Sie nach der Erstellung des Berichtprofils ein oder zwei Minuten lang. Der Bericht wird im Berichtverlauf angezeigt. Wenn der Bericht dennoch nicht erstellt werden kann, öffnen Sie das Berichtprofil, und speichern Sie es erneut. Falls das Problem weiterhin besteht, wenden Sie sich an den Trend Micro Support.

Weshalb kann ich keine täglichen/wöchentlichen/monatlichen Berichte per E-Mail erhalten, auch wenn sich Berichte im Berichtverlauf befinden?

Stellen Sie sicher, dass die E-Mail-Adresse des Kunden gültig und in der Liste der Empfänger für Berichtprofile enthalten ist. Sollte es daran nicht liegen, kann es sich um ein Netzwerkproblem handeln.

Warum werden Uhrzeit und Datum in einem erstellten Bericht nicht in meiner Zeitzone angezeigt?

Die Zeitzone, die im Bericht angezeigt wird, entspricht der vom Reseller ausgewählten Zeitzone bei der Profilerstellung. Sie wird nicht durch den Kundencomputer festgelegt.

Was bedeutet "n. v." nach der Erstellung eines Einzelberichts?

Bei Einzelberichten zeigt die Spalte Status stets "n. v." an. Weil ein Einzelbericht keinen Status aufweist (er kann nicht deaktiviert, aktiviert, unterbrochen werden usw.).

Bei der Verwendung von SSL- (HTTPS-) Verbindungen werden keine Berichte angezeigt.

"Verschlüsselte Seiten nicht auf der Festplatte speichern" ist eine Sicherheitseinstellung für Internet Explorer 7.0 / 8.0, die bei SSL-Verbindungen (HTTPS) verwendet wird. Wenn diese Einstellung markiert ist, werden keine Daten zwischengespeichert, und Berichte können weder geöffnet noch heruntergeladen werden.

Um diese Einstellung in IE 7.0/8.0 zu ändern, klicken Sie auf **Extras** > **Internetoptionen** > **Erweitert** > **Sicherheit** und deaktivieren Sie "**Verschlüsselte Seiten nicht auf der Festplatte speichern**".

Kapitel 12

Hilfe anfordern

Dieser Abschnitt enthält die folgenden Themen:

- *Kontaktaufnahme mit Trend Micro auf Seite 12-2*
- *Problemlösung beschleunigen auf Seite 12-2*
- *Support-Portal verwenden auf Seite 12-3*
- *Enzyklopädie der Bedrohungen auf Seite 12-3*
- *Info über Trend Micro auf Seite 12-4*
- *TrendLabs auf Seite 12-5*

Kontaktaufnahme mit Trend Micro

In Deutschland erreichen Sie unsere Trend Micro Vertriebspartner telefonisch, per Fax oder E-Mail:

Adresse	Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland
Tel.	+49 (0) 811 88990-700
Fax	+4981188990799
Internet-Adresse:	www.trendmicro.de
E-Mail:	support@trendmicro.com

- Weltweite Support-Büros:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Dokumentation zu Trend Micro Produkten:

  http://docs.trendmicro.com/de-de/home.aspx

Problemlösung beschleunigen

Zur Verbesserung der Problemlösung sollten Sie folgende Informationen bereithalten:

- Schritte, um das Problem nachzuvollziehen
- Angaben zur Appliance oder zum Netzwerk
- Marke und Modell des Computers sowie zusätzliche Hardware, die an den Endpunkt angeschlossen ist
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Version des Betriebssystems und des Service Packs
- Endpunkt-Client-Version

- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventuell erhaltener Fehlermeldungen.

Support-Portal verwenden

Über das Trend Micro Support-Portal können Sie rund um die Uhr online auf die aktuellsten Informationen über allgemeine und ungewöhnliche Probleme zugreifen.

Prozedur

1. Gehen Sie zu http://esupport.trendmicro.com.
2. Wählen Sie ein Produkt oder einen Service im entsprechenden Listenfeld aus und geben Sie andere damit verbundene Informationen an.

   Die Seite **Technischer Support** wird für das Produkt angezeigt.
3. Mit dem Feld **Support durchsuchen** können Sie nach verfügbaren Lösungen suchen.
4. Wenn keine Lösung gefunden werden konnte, klicken Sie im linken Navigationsbereich auf **Supportanfrage erstellen** und geben Sie alle relevanten Details ein. Sie können auch hier eine Supportanfrage erstellen:

   http://esupport.trendmicro.com/srf/srfmain.aspx

   Das Problem wird von einem Support-Mitarbeiter von Trend Micro untersucht, der innerhalb von 24 Stunden oder weniger auf Ihre Anfrage reagiert.

Enzyklopädie der Bedrohungen

Die meiste Malware besteht heutzutage aus "komplexen Bedrohungen" – zwei oder mehr miteinander kombinierte Technologien, um Computer-Sicherheitsprotokolle zu umgehen. Trend Micro bekämpft diese komplexe Malware mit Produkten, die eine

benutzerdefinierte Schutzstrategie erstellen. In der Enzyklopädie der Bedrohungen wird eine umfassende Liste mit Namen und Symptomen für verschiedene komplexe Bedrohungen, einschließlich bekannter Malware, Spam, bösartiger URLs und bekannten Sicherheitslücken, zur Verfügung gestellt.

Gehen Sie zu http://www.trendmicro.com/vinfo/de/virusencyclo/default.asp, um weitere Informationen über Folgendes zu erhalten:

- Malware und bösartige mobile Codes, die zum jeweiligen Zeitpunkt aktiv oder im Umlauf sind
- Seiten mit zusammenfassenden Informationen zu Bedrohungen, aus denen sich die gesamte Webangriffsgeschichte zusammensetzt
- Beratung zu Internet-Bedrohungen über gezielte Angriffe und Sicherheitsbedrohungen
- Informationen zu Webangriffen und Online-Trend
- Wöchentliche Malwareberichte.

Info über Trend Micro

Als weltweit führender Anbieter für Cloud-Sicherheit entwickelt Trend Micro Lösungen für die Bereiche Internet-Content-Security und Bedrohungsverwaltung, die Schutzmaßnahmen für den Austausch digitaler Daten zwischen Unternehmen und Kunden bieten. Mit über 20 Jahren an Erfahrung zeichnet sich Trend Micro durch erstklassige Client-, Server- und cloudbasierte Lösungen aus, mit denen Sicherheitsbedrohungen schneller gestoppt und Daten in physischen, virtuellen und Cloud-Umgebungen geschützt werden können.

Beim Auftreten neuer Bedrohungen und Schwachstellen ist Trend Micro auch weiterhin entschlossen, Kunden dabei zu unterstützen, ihre Daten zu schützen, Compliance zu gewährleisten, Kosten zu reduzieren und die Integrität der Unternehmen zu sichern. Weitere Informationen finden Sie unter:

http://www.trendmicro.com

Trend Micro und das Trend Micro T-Ball-Logo sind Marken von Trend Micro Incorporated. In einigen Rechtsgebieten handelt es sich dabei um eingetragene Marken.

Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken der entsprechenden Unternehmen.

TrendLabs

TrendLabs℠ ist ein weltweites Netzwerk von Forschungs-, Entwicklungs- und Aktionszentren, das rund um die Uhr Bedrohungen überwacht, Präventionsstrategien entwickelt sowie zeitnahe und nahtlose Lösungen liefert. Bei TrendLabs, das Rückgrat der Service-Infrastruktur von Trend Micro, sind mehrere hundert Mitarbeiter und zertifizierte Support-Experten beschäftigt, die sich um die vielfältigen Anfragen zu Produkten und technischem Support kümmern.

TrendLabs überwacht die weltweite Bedrohungslandschaft und liefert effektive Sicherheitsmaßnahmen zum Erkennen, Verhindern und Eliminieren von Angriffen. Die Kunden profitieren von diesen täglichen Bemühungen in Form von häufigen Viren-Pattern-Updates und Erweiterungen der Scan Engine.

Weitere Informationen über TrendLabs finden Sie unter:

http://www.trendmicro.de/newsroom/faces/index.html

Stichwortverzeichnis

S

Support
- Knowledge Base, 12-3
- Probleme schneller lösen, 12-2
- TrendLabs, 12-5

T

Textkonventionen, viii

TrendLabs, 12-5

TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraβe 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799 info@trendmicro.com

www.trendmicro.de

Element-Code: APGM36800/141125